Political Expression in Web Defacements

Thesis presented by

Michael Kurzmeier

in partial fulfilment of the requirements for the degree

of Doctor of Philosophy

Maynooth University

Centre for Digital Humanities / Department of Media Studies

09 / 2021

Supervision: Dr. Kylie Jarrett, Dr. Órla Murphy (UCC)

Acknowledgements

This dissertation would not have been possible without the patient support of many. I would like to thank the supervisory team of Dr. Órla Murphy (University College Cork) and Dr. Kylie Jarrett (Maynooth University) for embracing this unusual topic and taking on the hard work of transforming it into the scholarly work it is now.

For the support and encouragement both in teaching and conference hosting, I must also thank the Maynooth University Media Studies department and the Centre for Digital Humanities as well as the Research Development Office. Much of the professional development alongside of this thesis is owed to their support.

The Irish Research Council generously supported this project through a postgraduate scholarship, for which I thank them. Their support enabled me to carry out my research with a level of financial stability and security uncommon in postgraduate students.

For all the academic success I achieved on this journey, I owe the greatest debt of gratitude to fellow researcher and human Sharon Healy. It was her selfless support and encouragement that made all of this possible.

Almost all material essential to this work is found in community-based archives. I need to thank all hobbyist web archivists, data hoarders and unpaid webmasters for preserving the source material of this study.

For the long-standing personal support during this project I must thank my parents on whose unwavering support I could count on throughout the entirety of this project. I must finally thank my fiancée Frederique Masson for being by my side throughout all of it.

Acknowledgement of Funding:

This research project was funded by the Irish Research Council under grant GOIPG/2019/2303

IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn
www.research.ie

Abstract

The idea of influencing public opinion through digital media is ubiquitous, yet little is known about its origins. This thesis investigates the use of political communication through hacked websites. It is at the same time an exploratory description of the research tools and methods needed to find and retrieve such material.

The dissertation frames political expression through hacking as interference with the strata of digital communication and positions it within a larger history of on- and offline activist practices. The methodological section describes the difficulties of finding and accessing defaced pages, which are almost exclusively held by community-based archives. Based on already available and added metadata, the dataset of defacements is surveyed and topics, periods of high activity and prominent defacer groups are identified. Modes of expression are tracked to give insight to possible defacer motivation. This survey then serves as the basis for the following analysis of two emblematic clusters of activity: The Kashmir conflict and the 9/11 attacks. In a close reading of selected defacements, communication strategies and general types of defacements are described, thereby showcasing the diversity of defacer standpoints and strategies which runs counter to the common uniform depiction of hackers. The notion of defacements as forced injection of material into a public sphere is discussed throughout these close readings and leads to the final analytical section discussing the relation between defacements and WikiLeaks.

After reflecting on the themes that unite this dissertation, the conclusion reflects on the preservation and availability of source material on defaced pages. The author expresses the hope that both the research methodology as well as the applied analyses will promote the understanding of web defacements as a resource for inquests into online political expression.

Table of Contents

Table of Tables

Table of Figures

1. Introduction

The term web defacement describes the unauthorized alteration of a web page, usually achieved through illicit access to the hosting server. The prefix web implies a lineage of practice from offline to online defacements and situates web defacements in a wider realm of activism. The fact that illicit access is central to being able to deface a web resource also suggests that a specialized set of skills is necessary to be able to participate in web defacements. This again implies that the topic branches out into the general realm of hacking and the organization of knowledge related to hacking. This intersecting moment of political expression and technical expertise defines the object of this dissertation.

Specifically for the context of this study, engagement with public discourse, introduction of material into public discourse and online commemoration of events in defacements were in focus. These web defacements are part of the larger realm of hacktivist and web defacement practices. As defaced pages are generally short-lived, research cannot rely on larger, unspecified Internet archiving services to obtain copies, nor can it follow events in real time. Defaced pages are recorded in community-built and maintained cybercrime archives, from which most of the data for this research has been sourced. This dissertation is thus a study of two elements – the web defacements themselves and the archives and archiving practices.

People try and find the hidden possibilities of electronic systems for all sorts of reasons; as part of their profession, as a personal interest, for their own gain or in pursuit of a higher goal. The expressions produced by these hackers are as diverse as their methods and motivations. While the exact scope of this study and the possible motivations of defacers will be subjects of coming chapters, it is at this point important to refer back to the thesis' title and declare that only defacements making specific and overt political claims are in scope for the following analysis.

The choice of political expression in defaced websites as a research object for this study serves three main purposes:

First, it explores a part of online subcultural history. It traces trends, actors, platforms and lineages of the defacer scene and brings to light an under-reported aspect of this community. By providing a quantitative analysis of modes of expression and communication over time, the study produces a data-based survey of defacer activity such as targets over time, modes of communication and the nature of the declaration. This is done with the intention to identify more about the nature of this subculture.

Second, in focussing on the political expression of web defacements, the study emphasizes the competitive scenario defacements take place in. Defacements per se compete over the limited resource of attention. The stabilizing and multiplying function of the archive is likely one of the key motivators behind any community-maintained cybercrime archive, making it valuable for understanding both the politics and the competitive media and subcultural environment in which these defacements take place. If the focus is set on how defacements attempt to interact with a public in the broadest sense, the acts of overwriting and occupying digital space in pursuit of communicative effects are brought to the fore.

This competitiveness and the overwriting of digital text is what gives this thesis most of its theoretical foundation. Interwoven into the chapters and arguments is the rejection of a digital exceptionalism. Rather than understanding the Internet as a boundless space distinct from the mechanics which govern other media, this thesis reads the digital as a complex system of material components arranged and governed by the social system which produced it. It understands hacking as antagonistic writing of electronic text, as an act of accessing stored information and overwriting them much in the same way as interjected pieces of memory are meant to overwrite their competitors. For this reason, the term digital media is used sparingly throughout this thesis as it tends to invoke ideas of something radically different and new. In much the same way that hacktivism is seen as the product of a lineage of political thought and practice, digital media is seen as the product of a lineage of previous electronic and physical media. Instead of digital, this thesis often uses the term electronic media or highly integrated media. In line with this, the argument is that most electronic and all digital media rely on an interface to be accessible to the human observer. Levels of integration (i.e. the dependence on the interface and the complexity of it) vary between different forms of media. What these media share, however, is that they are at their core machine-to-machine communication with the realization through the interface only being an optional last step. This reliance on the facilitating infrastructure also opens up a new way of engaging with the media's source code. Hacking does exactly that: it engages with the otherwise hidden source code of that system. Defacements are a subsection of that hacking with a more specific purpose.

Third, this thesis is an advocacy for web archiving and an effort to preserve the contested history of attempts to partake in a public debate online. Defacements are at a double disadvantage in regard to their preservation. On a technical level, defacements are more ephemeral than most other types of websites. Seen as unwanted and often illegal intrusions into computer systems, defaced pages tend to be restored or taken offline before large Internet archiving crawls can find them. Socially, defacements are often regarded as nuisances rather than artefacts worthy of cataloguing and consideration.

But it is not only the defacements that are at risk. For all the work computer security enthusiasts have invested into building and maintaining the community-based archives used in this study, these archives are at risk of disappearing. Building on previous work on defacements, this study has already found many of the mentioned collections turned into error 404 – file not found.[1] Surprisingly, it is

[1] This topic of irretrievable original sources runs throughout the thesis. Were possible, original sources were used and their URLS archives through the Internet Archive. In some cases,

exactly the community aspect of hacking which has allowed some defacements to become part of an archive and to survive until today. As the following chapters will to show, defacers submitted their works to one of the archives in order to build reputations as skilled hackers. From the oldest known defacements in 1996 to the one archive still actively collecting pages today, the social aspect of computer culture, hacking and defacement communities is what has led to the establishment of the infrastructure which in part will be the object of analysis in this thesis. As most of these archives have stopped accepting new submissions or have gone offline altogether, it seems to be only a matter of time until most of the source material for the study of defacements is gone from the web. Because of this imminent loss of material, an important section of the study will discuss methods of finding, retrieving and sorting this type of data.

Implied in this advocacy for web archiving is the delivery of a metadata system to adequately describe and thus make defacements useable for academic research. As in many web archiving efforts, the problems arising from a large collection of unrelated, unstructured data are problems of identifying relevant material within the corpus and problems of making adequate and data-based statements about themes and sentiments within that corpus. As a first step towards a larger-scale academic engagement with defaced web pages, this thesis also presents methods for the investigation of large collections of web pages with a focus on the specificities of defacements.

The above has argued against digital exceptionalism and for an understanding of electronic media as a continuation of existing technologies and practices, obscured by their own mythology. These mythologies obfuscate the understanding of electronic media. To counter these tendencies, the literature review follows a historic approach to the development of the understanding of hacking practices inspired by Streeter (2011), Parikka (2015) and Zielinski (2006). This approach is not one of nostalgia, but one of rooting attitudes towards defacements in the material conditions of society. It thus follows not a timeline of inventions in a teleological explanation of the current, platformized web, but it attempts to find moments where attitudes towards technology and technology's application in society changed.

To further demystify digital media and lead into the topic of network interference, consider the below map (Figure 1.1) of submarine cables connecting countries to a communication network, part of which is what is commonly called the Internet:

This map offers rich reading in terms of inequalities of access (if one was to count individual country's connections), yet also visualizes the physicality of a global communication network. At this high level, it is a common understanding that control over parts of this network is an important asset. Admiral James Stavridis,

where the site would not allow archiving crawls to run, a local copy was created. Where original sources were not or no longer available, archived material was used instead.

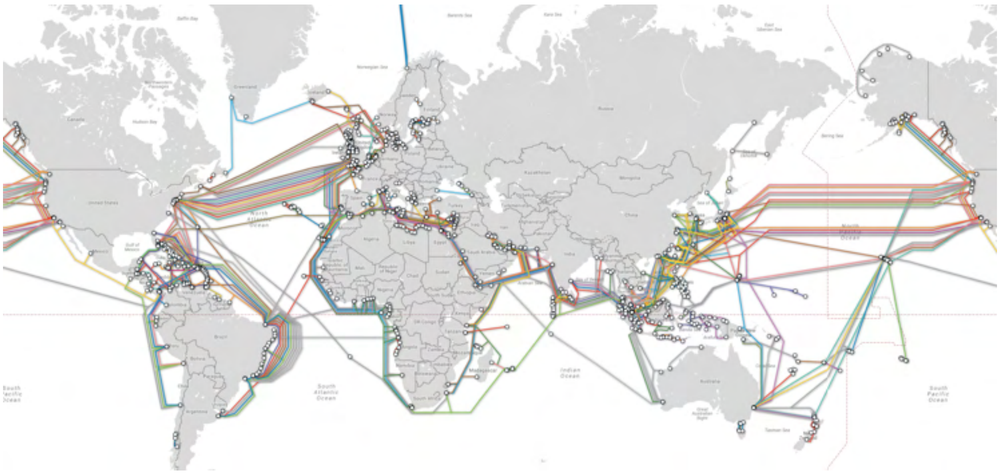


Figure 1.1: Submarine cable connections, from Dormon (2016)

former NATO Supreme Allied Commander Europe, assesses attacks on the physical infrastructure of the Internet as likely and devastating:

> … the technical capabilities required to damage cables are relatively low and unsophisticated. The risk posed to these garden hose-thin connections that carry everything from military intelligence to global financial data is real and growing. In the most severe scenario of an all-out attack upon undersea cable infrastructure by a hostile actor the impact of connectivity loss is potentially catastrophic, but even relatively limited sabotage has the potential to cause significant economic disruption and damage military communications. (in: Sunak, Stavridis, and Policy Exchange (Think tank) 2017, 9)

This fictional scenario of enemy vessels destroying undersea infrastructure is complemented by the report of a much less sophisticated attack on the facilitating infrastructure which took place in California in 2009:

> This example of cable severing is important to note because it happened on land – a restatement to the fact that cables are also vulnerable when they emerge from the ocean. Ten cables were cut in what is thought to be a case of vandalism. It is notable that, at the time, it was observed that the perpetrators simply had to lift an unsecured manhole cover and, once they had climbed down the ladders, merely cut the cables with pliers. This straightforward, unsophisticated act of vandalism led to 1.5 million services being disrupted, including all ATM and credit card processing in the area of Southern California. Further to this, 52,000 landlines operated by Verizon were completely disconnected. (Sunak, Stavridis, and Policy Exchange (Think tank) 2017, 38)

Both sections confirm observations about digital media's special relationship with their facilitating infrastructure where a configuration of cables and servers constitute another stratum to engage with. The California example is especially significant as it seems to be the exact type of attack on global communication infrastructure discussed later in this thesis.

On this high-level overview, it seems clear that the physicality of the Internet is a factor which shapes its content – and that a pair of pliers can bring down millions of services on an allegedly decentralized network. If those intercontinental connections are the highest level, national efforts to stir in the stratum – affect the flow of information in and out of a country and are more targeted than the destructive interferences described above. As an example, consider recent partial Internet shutdowns in Tanzania:

> Starting from yesterday (27th October 2020) – *on the eve of Tanzania's 2020 general election* – OONI [Open Observatory of Network Interference] measurements continue to show the ongoing blocking of social media (and of the Tor circumvention tool) in Tanzania. (Xynou 2020)

Consider as well a total shutdown in Uganda, also related to elections:

> [A]mid its 2021 general election, Uganda was disconnected from the internet entirely. The country experienced a widespread internet blackout that lasted 4 days, starting on the eve of the election (13th January 2021) and ending in the morning of 18th January 2021. In the days leading up to the election, access to major social media platforms and circumvention tools was blocked. (Xynou et al. 2021)

So far, this cursory exploration has shown that control of the infrastructure is considered a valuable asset from a multitude of perspectives. This control ranges from destruction (NATO assessment, California incident) to total shutdown (Uganda), to a partial shutdown (Tanzania). Added to this list can be instances of hacktivism such as:

> January 1997: Visitors to www.plannedparenthood.com are greeted with the words, "Welcome to the Planned Parenthood Home Page!" above an ad for the anti-abortion book, "The Cost of Abortion." The web site is operated not by Planned Parenthood, but by anti-abortion activist Richard Bucci.

And:

> June 2000: Visitors to nike.com find themselves reading information about the problems of global capitalism. Nike's web site has been redirected to the web site of s11, an anti- globalization group. (Both in: Samuel 2014, 1)

Trends that emerge from this incomplete compilation are twofold:

> Flows of information are valuable targets for one, and vulnerable assets for the other side. Manipulation is possible by interference with the physicality of the underlying infrastructure, be it cutting cables or exploiting vulnerabilities in servers. Manipulation can take the form of total disconnection, partial shutdown (which potentially increases the impact of other media) and alteration which combines surprise and disruption)
>
> The more small-scale an interference with these flows is, the more fine-tuned it can be. Submarines and pliers destroy the infrastructure which enables these flows hackers can alter websites.

This positions hackers in a greater context of what may be called "strategic interference". The trends mentioned above argue against any form of exceptionalism and for understanding hacking as one of many strategies to influence the stratum of communication. Hacktivists in general, and web defacers in particular are at the bottom of this hierarchy as their interference tends to be small-scale and targeted. This is not to say hacktivism has no influence, but rather to draw the line between digital vandalism and digital activism and to emphasize that web defacements and hacktivism must be seen as the result of a lineage of thought and practice.

Starting with the study object – hacktivism – the literature review identifies five distinct influences/subcultures the understanding of hacktivism draws upon:

- Counterculture with its disdain for centralized structures and technocracy plus a favourable attitude towards the re-appropriation of technologies.
- Computer culture which helped shape the hacker identity, and led to dedicated computer and online policies.
- The open source movement which introduced ideas of digital commons and free software.
- Culture Jamming as a Situationist practice to subvert mainstream narratives and images and re-appropriate media in public spaces.
- Cyberspace, the concept of a media network as a worthwhile and meaningful place of human interaction.

Through this history of hacktivism, a historic perspective on the development of both defacers, their targets and their audience can be developed. This perspective also forms the basis for a critique of existing literature on the study object.

The study was complicated by the absence of a universally accepted definition of, and a multitude of perspectives employed on, the topic of web defacements. Engagement with the subject comes from IT security, social studies, art, legal, and a range of related disciplines. Nevertheless, there were few sources for exploring web defacements specifically. Political expression in web defacements had seen few dedicated studies and the relation between public sphere communication and digital media had seen some engagement in a Foucauldian tradition, yet little material was available on the effects of the materiality of information in digital media. In other words, the connections between the hardware, the software and the user interface output – often enough the preferred attack vectors for hackers – were under-researched.

When referring to obfuscating mythologies around digital media, the most prominent is the alleged boundlessness of the digital. On the basis of the claim that data has no physical substrate is implied that data is boundless, not subject to resource scarcity and thus has no need for regulation. The thesis' section on the materiality of the Internet employs Barthes' concept of myth as a second-order-process (2006) to analyse the role and influence of material on electronic media. It establishes hacking as a material practice, as an antagonistic writing of electronic text, as the change in stored bits, and the change in control over one or many machines.

In doing so, it connects back to the concept of electronic media as machine-to-machine communication. Dealing with information in the context of electronic media then opens up two possibilities of interference for the hacker: One, the machine-to-machine communication itself which may be interfered with – hacked – and second, the content of the site which, through over-writing existing 1s and 0s on a hard drive, change the content of the Barthesian meaning-making process. The analysis will show how defacers utilize this process to maximise the impact of their defacements.

Following this, the method used to capture and analyse data on the defacer archives is described. The methodology of this study had to account for the distributed and fragile nature of the collections in question, the lack of descriptive metadata and the lack of best practice models for the analysis of hacked websites. Further, as websites unwillingly become targets of defacements, additional ethical considerations had to be factored into the research design. The employed method can be broken into two parts: acquisition of material and analysis.

It is at this point necessary to issue a word of warning: in many cases, random thrown-together file dumps somehow relating to defaced websites use the term "archive" for themselves. This attribution is almost always wrong. The so-called archive this thesis builds upon is called Zone-H and holds upwards of 3 million defaced pages with virtually no way to search, group or filter content. Adding to this problematic is the ephemerality of Zone-H and other, similar archives. This thesis advocates for, and carries out some of the work of, removing the quotations around archive – meaning to turn ephemeral file collections into academic (meaning stable, accessible and queryable) resources.

Before any further discussion of the content, it must be acknowledged that the focus on a single source of information brings with it the risk of reproducing the source's bias. While the actual collection practice of Zone-H remains unknown, it is safe to assume that the site's competitive nature appealed to some defacers more than others and that only those who saw merit in Zone-H's work would submit their own defacements to be archived. Limitations also extend to the field of language, solely focussing on the English language brings with it the risk of omitting defacers speaking to and from other cultures. These limitations must be kept in mind, especially when discussion any assumed political orientation amongst defacers. Both the ethics and the methodology chapter will discuss these in detail.

The acquisition step required finding a solution to the fact that Zone-H as the largest source of defaced websites accepts all sorts of defacement and not only political content. While it offers a rudimentary search function, users can not search the content of pages, only the domain and the name of the defacer. Furthermore, the site uses JavaScript which means it cannot be crawled by common web crawlers and thus no copy of it exists in larger collections such as the Internet Archive. Zone-H requests captchas[2] after around 80 pages and temporarily bans the user after viewing around 800 pages. Using a self-developed automated browsing solution and patience, 12,000 defaced pages were extracted from the archive in a semi-automated approach. The program was designed to start at the oldest defacements and attempt to browser the archive one by one until the daily ban occurred.[3] Captchas still had to be resolved by hand which required constant supervision of the process. Once the capture was complete, data was screened for political web defacements.

Analysis of the data was a somewhat more pleasant process. Using the time and date of the defacement, defacer name and the affiliation of the target site (governmental, institutional or random target), defacements were clustered into periods of high activity and defacer groups were traced over time. This grouping presented the basis for the selection of two distinct time periods for web defacements; the Kashmir conflict which mostly saw Pakistani hackers deface Indian and Western websites and 9/11 which saw a wave of expressions of solidarity with the US.

The first part of the analysis is a quantitative overview of the research dataset. This chapter is based on two different data sources, one being the metadata recorded during the capture progress and the overall yearly statistics released by Zone-H. The other data source is manually derived from the individual pages and includes the type of defacement, mode of expression, occurrence of elements of internal and/or external communication, explicit claims of group membership and explicit messages to whoever is seen as the enemy.

The rationale for contrasting metadata from the in-scope defacements to the overall yearly statistics was to investigate whether political defacements are in any way different from regular defacements and if that difference could be described in metadata. One of the key points here was the choice of targets. Authors have described how political defacements tend to be more selective about their targets (Samuel 2014; Maggi et al. 2018; Balduzzi et al. 2018), so that political defacers are more likely to target more difficult, but more high profile sites such as governmental institutions' pages. This seems plausible, and in fact some of the oldest available material on political defacements dates back to August (US Department of Justice) and September (CIA) of 1996.[4] To be able to make a

[2] "A CAPTCHA (short for Completely Automated Public Turing Test To Tell Computers and Humans Apart) is a program designed to secure websites from automated bot attacks and spammers by generating a test that humans can pass but computers cannot." (Carnegie Mellon University CyLab 2017)

[3] This hard-to-access design is not the result of bad user interface planning. Following a reference by Balduzzi et al. about purchasing a copy of the full archive (2018, 2), I contacted the admin of Zone-H with the intention to find out if this was indeed the site's business model. I received a quote of CHF 12000 for the full dataset. It seems likely that one of the reasons the site is still around is the value it holds. I did not continue the negotiations.

[4] These defacements are held by Attrition.org, which has since stopped accepting new submissions and removed the archive from the public web. Thanks to Jericho, one of the admins, I was able to receive a full copy of the archive for research purposes. A mirror of the two mentioned defacements is available.

quantitative statement about whether this was the norm or the exception, this first part of the analysis will use the available, general metadata on defaced pages, targets, operating systems and the like and turn it into a basis against which the specific metadata collected from political web defacements can be compared. Implied in “profiling” defacements in this way is also the question of scalability of this study, so that in a hypothetical scenario relevant content could be found in the dataset through the metadata.

Building on the contrasting of metadata, the content of the defacements itself was analysed using Natural Language Processing (NLP). This approach allows the identification of common word combinations and word frequencies. Similar to how the approach to metadata helps to identify political web defacements, the NLP-driven approach helps to find the most commonly talked about events, the most commonly used words and word combinations.[5] Through this process, key topics could be established and individual defacements selected for closer analysis. The advantage of this method is that it grounds the individual case studies well within the larger corpus so they are truly emblematic of larger trends. The NLP-based approach also allows scaling up of this project and can be repeated with almost any size collection.

The question of defacer motivation will come up time and again throughout the design of this study. Why would individuals spend time and effort, and risk persecution as hackers, to leave messages on defaced pages? I can at this point refer to the work of Alexandra Samuel who in her 2004 thesis interviewed defacers to investigate their motivations to produce a qualitative study of defacer motivation. As much as her work in many ways was a source of inspiration for this thesis, my approach was to be able to arrive at a data-driven insight into defacer motivation. This was partially because sources disappear and defacers are harder to find and contact, and partially because I wanted to survey a larger corpus.

After the metadata comparison has created a profile of political hacktivism and after NLP has identified clusters, topics and sentiment, the first part of the analysis will then dive deeper into the available material and manually code elements indicative of defacer motivation. One strength of this approach is that it accounts for the diversity and heterogeneity found in the research data set. As much as there is no one type of defacer, there is no singular motivation in defacing. From extensive work with the research dataset, what drives people to participate in this activity is as diverse as their backgrounds and can range from a desire to participate in a public discussion the defacer feels outed from, an expression of anger of grief or a passing remark in an otherwise non-political defacement.

[5] Just as for me, English is not a first language for many defacers. Unlike in my case, defacers cannot rely on professionals to review their work to catch the worst grammar and spelling mistakes. Non-standard spelling can help the analysis – when words are always spelled a certain way in a certain context – or obfuscate when spelling varies from case to case. When excerpts from defaced pages are reproduced in this thesis, the original spelling is reproduced.

Motivations can intersect, overlap and even contradict each other, as the analysis will show in detail. To mention just one example, the desire to communicate to an outwards (non-hacker) audience can be in conflict with the desire to also receive recognition from an insider (hacker) audience by using the appropriate references, sending out greetings and using insider codes. This tension between conflicting motivations which is sometimes felt in defacements is acknowledged and represented by this multi-layered approach to defacer motivation. The analysis of communicative elements will also touch upon themes of community building and maintenance when it codes different instances of referring to fellow actors in the defacement scene. These references can take the form of greetings, expressions of approval and disapproval, declarations of adherence to what the author perceives as scene-internal rules or, likewise, accusations that other defacers have broken some of these rules. These references and features are going to be monitored over time and taken as indicative of defacer motivation.

In tracing these motivations over time, a conclusive picture of subcultural practices, modes of expression and communication (more internal or more external) and direction of communication (more directed at a public or more directed at an enemy) emerges. The analysis will show that the web defacement scene underwent changes over time, how memorial and narrative-based defacements replace informative and argumentative defacements and how scene-internal references become less common. This background of framing the dataset through metadata, identifying topics through NLP and finally describing motivations and incentives over time provides a strong support to zoom in even more and enter an in-depth reading of selected defacements.

The conflict between India and Pakistan over the Kashmir province and its related defacements have been selected for close reading in Chapter 6. The focus of that chapter will be the communicative function of defacements and will refer back to questions posed in Chapter 5 about the inward or outward direction of communication in defacements. At the same time, the chapter serves as an extended introduction into the practicalities of web defacements. It adds selected defacements as emblematic representations to the thesis' theoretical framing of defacements and their facilitating infrastructure.

It was earlier suggested that a certain tension between communicative modes and a struggle for the right and most effective form of expression is sometimes palpable in defacements, and examples from the Kashmir cluster are where this tension is best observed. Analysing the visual elements used in selected defacements, the chapter will show how defacements from this period follow a tripartite structure of header-body-footer, with each element having distinct communicative functions and audiences.

Most of the defacements from the Kashmir cluster date to the early 2000s and, despite being sometimes framed as a cyberwar between India and Pakistan, they are almost exclusively written from a Pakistani perspective with the intent to (sometimes) insult and ridicule Indian politics and government or (more often) to speak to a Western audience with a plea for help. In doing so, defacements from the Kashmir cluster are mostly meant as contributions to a public debate defacers assume Western politics to be based on. This attempt to partake in public debate through web defacements, and how defacers attempt to make the Kashmir conflict part of a Western collective memory will be analysed in detail in this section. Only one known defacement speaks critically of Pakistan's involvement in the conflict, and this defacement is at the same time the most advanced in its communicative strategy. The defacement, which replicates an interview, takes a step forward in that it does not attempt to break into an imaginary discourse, but attacks the credibility of the Pakistani narrative of their role in the conflict as a whole. In doing so, this defacement is an important bridge away from a small-scale and argumentative, and towards an emotional approach in defacements.

Chapter 5 is complemented by a selection of primary sources on the largest and most active defacer groups in the Kashmir cluster. Both groups' homepages were preserved and reveal further information about the image and motivations of defacers at the time. Additionally, interviews with one of the group are available which will give further insight into their structures, motives and backgrounds. This material complements the analysis without replacing it or shifting the focus of the thesis. Yet it shows the publicity sought and enjoyed by defacers and confirms findings from the close reading about the – assumed and real – communicative function of their work.

What emerges in both the close reading of the primary material on defacer groups is the competitive aspect of defacements: a defacer's quality is measured by the amount of attention he/she can hijack. This indicates defacers are acting in an attention economy. What happens when that economy is shaken up and the usual market rules and tactics need to be re-invented is shown in Chapter 6 which investigates the cluster of 9/11-related defacements.

The attacks on the World Trade Center on 11th of September 2001 are in many regards seen as a caesura in Western societies. For web defacements, the events led to a dilemma which required a reconfiguration of defacer image and message. Referring to the attention economy defacers operate in, almost all public attention was absorbed by the events and their political fallout. Defacers had to adapt to this by making 9/11 a topic in defacements, without alienating their Western audiences. They did attempt to solve this dilemma through increased use of a memorial-type defacement that, instead of breaking into a discourse, now attempts to participate in an empathetic public's grief. As Chapter 4's data analysis has already hinted, 9/11 is when memorial-type defacements become the most commonly used type of defacements. The chapter will show in detail how different strategies of this approach work, from forcing viewers to re-experience the images to establishing one's own position by publicly participating in grief.

The second challenge 9/11 brought to defacers was the increased pressure they found themselves under following tightened security legislation. The trope of wrongful persecution through an ignorant public runs deep in hacker culture and was brought to new life through the *Patriot Act* which expanded definitions of cybercrime.[6] The chapter will show how defacers emphasized their own harmlessness, even insignificance and largely declared their allegiance to general US politics post-9/11. The general pro-US tone of the 9/11 defacements might seem surprising at first – there is only one dedicated anti-US defacement found in the cluster – but the chapter will show how this attitude is in line with the lineage of hacktivism as described in the theoretical framework and with the communicative function of defacements being directed at a Western audience.

Defacements in Chapter 6 are generally more diverse than those from the Kashmir cluster, with less primary material available on defacer groups. The examples presented in the chapter have thus been selected to represent this diversity of styles. Since one group of defacers was active in both the Kashmir and the 9/11 cluster, their activity profile will be compared across the two clusters to further understand how defacement campaigns are organized. Primary material is available on one group, yet not in the context of 9/11. The section will be complemented by an analysis of national symbols such as flags, coats-of-arms, and clear references to national origin in defacements as these elements are widely used throughout the 9/11 cluster.

When designing this study, it was quietly assumed that WikiLeaks as the most well-known hacktivist platform would have seen larger-scale coverage in web defacements. This assumption was made since web defacements are a hacktivist practice. Following a lineage from 9/11 to the invasions of Afghanistan and Iraq to the respective leaks of documents, WikiLeaks appeared to be a certain topic of defacements. In fact, very few defacements exist that mention WikiLeaks at all. Building on the arguments in Chapter 6, Chapter 7 investigates the complicated relation between defacers and WikiLeaks.

Chapter 7 concerning WikiLeaks will serve as an investigation into the relation between Zone-H as a platform, defacers as actors in an attention economy and WikiLeaks as an information capitalist. The section describes the few intersections between the three in the context of their different and at times opposing roles. Zone-H as a platform experiences a similar situation post-9/11 to that defacers found themselves in: while they enjoy a bit of notoriety, they do not want to be drawn into the political fallout by association. Zone-H consequently released a handful of statements declaring their non-involvement with WikiLeaks and expressing their function as a mere record of defacements.

Defacers as actors compete for the limited resource of public attention. That this competitive situation supersedes ideas of solidarity will be shown in cases where domains belonging to WikiLeaks were defaced not to oppose WikiLeaks but for

[6] See USA Patriot Act (u.s. H.r. 3162, Public Law 107-56) (n.d., sec. 814).

the attention the domain would receive. The value of the section lies in further showcasing the diversity within the defacement scene and challenging narratives of the hacker. What its results are going to show is that the competitive scenario of defacements leads some defacers to see WikiLeaks as unwanted competition while others feel the need to comment on WikiLeaks and its actions, either positively or negatively.

The wide range of research questions, methods, case studies and data within this thesis presents both challenge and opportunity. It is a challenge to adequately cover all technical, sociological, archival, and media-related aspects of the research object. This wide approach is necessary, however, to access the research object in its complexity and discover threads which run across multiple disciplines. Because hacktivism and web defacements are usually described through the eyes of one discipline only, this multi-angle approach allows us to gain new insight into the historical development of public debate through the Internet. It is at the same time a contribution to and an advocacy for the academic engagement with web archives.

2. Literature Review

2.1 Introduction

Hacking is a term best avoided in academic writing for how unclearly it is defined.[7] It is, however, not possible to talk about web defacements without first explaining the hacking scene they emerged from. Hacking is further complicated by the abundance of narrations and stereotypical depictions of hackers ranging from individualistic cyber-hedonists to faceless saboteurs of infrastructure working for monetary gain or in the interests of a perceived enemy nation.[8] Hacktivism on the other hand has been associated more positively with progressive and emergent social protest. It might thus be tempting to use the expressions hacktivism and hacking as if they could be described in isolation, without having to refer to any external frameworks.

However, hacktivism is a phenomenon embedded in power structures and technologies. Understanding of it is obscured by the narratives that surround it. The purpose of this literature review chapter is to document movements or schools of thought which have added to the current understanding of hacktivism. In line with the overall framework of the thesis which reads web defacements as activist practice facilitated through hacking, the literature review also takes into account how web defacements are situated within these larger topics.

In light of all this, it is necessary to begin with a conceptual understanding of hacking. This thesis understands hacking primarily as antagonistic writing of electronic text. Through this conceptualization, the implied connotation of hacking and hacktivism is reduced and through association with writing, the practices of hacking and hacktivism are more embedded into existing laws, conventions and design. A subset of this writing, in relation to the principles surrounding it, can be described as antagonistic in the sense that one act of writing overrides the other. Further down in this subset of writing, then, are acts of writing that are not only antagonistic, but violations of one or many of the surrounding laws, conventions and designs. Now we are approaching something that under certain circumstances might be called hacking. Motivations for this type of writing are diverse, but what drives all forms of antagonistic engagement with media is narratives of how media should be. Without this utopian vision, or without an actual cause of concern, none of these practices would be able to mobilize its supporters. With this in mind, the existing literature will be reviewed.

[7] For example, see the definition in Merriam-Webster for hack: “to gain illegal access to (a computer network, system, etc.)” (‘Hack’, n.d.) which only covers the question of access to a system and omits questions such as ownership, usage and licence agreements, copyright and method of access.

[8] Most recently, hacking is often understood in the context of the growing field of ransomware attacks, where attackers obtain control over the victim’s data (Palmer 2021). Ransom is then demanded for the decryption or non-disclosure of data, as in the case of the attack on the Irish Health Service (Jo Tidy 2021).

This brief history of hacktivism is an investigation into the ideological underpinnings of hacktivism at the time when the phenomena started to appear on the web. From there on, the chapter is going to establish how changes in the structure of the Internet have been reflected in hacktivist practices and how the idea of a web defacement came to be.

It is probably impossible to determine time and location of the very first page defaced in the context of hacktivism, but in accordance with the existing literature it seems safe to place the origins of hacktivism as a dedicated form of political activity in the second half of the 1990s. Although a notable hacking scene existed long before, and the expression cybercrime also was of no novelty, the 1996 hack of the US Department of Justice website can be seen as one of the first web defacements that combined hacking with political activism. The site itself was altered to protest the Communications Decency Act (CDA). An excerpt reads:

> Free speech in the land of the free? Arms in the home of the brave? Privacy in a state of wiretaps and government intrusion? Unreasonable searches? We are a little behind our 1984 deadline, but working slowly one amendment at a time. It is hard to trick hundreds of millions of people out of their freedoms, but we should be complete within a decade. "Site defacement, US Dept. of Justice" 1996 (qtd. in Samuel 2014, 9) [9]

This message, written more than two decades ago, brings with it two important questions regarding the origins of hacktivism. First, what are the historical conditions that lead to the formation of hacktivism? If we agree that hacking in the sense of unauthorized interference with electronic signal processing systems existed since the 1900s (Marks 2011) and, more specifically, computer network hacking existed at least since 1988 (Davis 2015), we have to ask why hacktivism appeared when it did and not at an earlier or later point in the history of electric communication. The answer to this I see in hacktivism’s emergence from four distinct subcultures and cultural movements that will be explored in the following.

The second question relates to the choice of medium. By the time the Department of Justice’s website was defaced, visual media existed for centuries, and electronic multimedia existed for decades. It seems strange that computer networks are so readily accepted as grounds for hacktivist activity, while other media is not. Radio and television, for example, have their own history of speech, counter-speech and culture jamming (as evident in pirate radio stations and live show trolling), not to mention leaflets, pamphlets and book censorship. These acts are acts of text production, that do not necessarily overwrite, but are in opposition to each other. In the context of electronic media, though, the act of overwriting becomes central to activism. This means that we can position hacktivism within a set of practices reacting to media. The answer to this question lies partly in the combination of cultural influences that lead to hacktivism, but also partly in the material

[9] The source mentioned by Samuel refers to a mirror page that is not available. This is often the case when researching hacktivism, as mirrors are often too slow to capture the defaced page before it is restored. Where possible, I am going to refer to the original source.

conditions of the medium, expressed partially in its tendency to break and its accessibility. The following chapters aim to describe these influences.

2.2 Hacktivism

Existing definitions of hacktivism in literature reflect on the phenomenon's position at an intersection between activism and hacking. Hacktivism’s influence on policy has been recognized by researchers since 1999 when Dorothy E. Denning described hacktivism in the context of the Kosovo War. The work, titled “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy” (1999), describes hacktivism as related to cyberterrorism and established forms of activism. This positioning of hacktivism at a middle ground between the other two phenomena has been adapted by later researchers.

For the context of this thesis, hacktivism will be defined as

the nonviolent use of illegal or legally ambiguous digital methods for political ends.

This definition borrows from Alexandra Samuel’s 2014 PhD thesis *Hacktivism and the Future of Political Participation.* The thesis is the first empirical study of individuals’ motivations to participate in this form of political engagement. Samuel defines hacktivism as:

> the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development. (2014, III)

This definition has been chosen with the intention of combining the two different strains of writing about hacktivism. A view on hacktivism as a potential external influence on politics and national infrastructure was central for writing on the topic during the early 2000s. While governmental agencies attempted to estimate the future influence of hacktivism (National Infrastructure Protection Center 2001), an early strain of activist literature emerged that was equally interested in the possible uses of digital activism. For instance, Tim Jordan in his 2002 book *Activism! Direct Action, Hacktivism and the Future of Society* describes hacktivism as “transgressions of the information infrastructures of 21st-century socio-economies” (2002, 121). Additionally, Mark G. Milone defines hacktivism as “surreptitious computer access or the dissemination of potentially disruptive and/or subversive software” (2002, 77) and advocates educating hacktivists on how even well-meaning intentions can cause damage to vital web infrastructure. Leah A. Lievrouw presents a more rigid definition of hacktivism as the reconfiguration of media itself and thus qualifies hacktivism as the work of (activist) computer professionals (2011).

Hacktivism is also associated with other forms of mediated activism such as culture jamming. Culture jamming is defined as

> a genre which critiques popular/mainstream culture, particularly corporate capitalism, commercialism, and consumerism. Here, media artists and activists appropriate and ‘repurpose’ elements from popular culture to make new works with an ironic or subversive point. (Lievrouw 2011, 22)

However, as the definitions by Jordan, Milone or Lievrouw suggest, hacktivism has a particular connection to information architecture and so its origins and politics must be looked for in the history of computing and computing cultures.

The reader may have noticed how the previous two sections aimed to describe first hacking, and then hacktivism. This was necessary because hacking and hacktivism are two overarching structures in which web defacements are embedded. As said in the introductory paragraph, it is tempting but hardly possible to draw clear lines between hacking as a cultural practice, activism in connection with technology and over-writing web pages. This is because hacktivism builds upon many different influences and traditions, many of them predating the Internet. This diverse lineage is why is necessary to develop this historical and cultural perspective to understand web defacements as they present themselves from a contemporary perspective. The countercultural influence described in the following section is probably the most historically distant. From there, the subject of web defacements will first be approached.

2.3 Counterculture

To investigate when forms of antagonistic writing of electronic text appeared on a significant scale, it is important to understand the origins of public debates about the relationship between technology and society. Even though the counterculture was not primarily a computer culture, it was a moment when debates about actual and potential technology usage attracted large audiences.

Steward Brand, the founder of the *Whole Earth Catalog*, is quoted as saying “computers might be the new LSD” (Turner 2006, 139). It is worth contextualizing this within the history of computer access. Firstly, both computers and LSD are reappropriated technologies that share a common history of very limited access to only a group of specialists and both were ultimately taken out of the lab and found widespread use in a scene that opposed those governmental institutions which enabled research on the technology. The “hardware” was introduced to a loosely organized scene that was interested in making use of it for self-determined and political purposes. This is further exemplified when considering how Brand’s *Whole Earth Catalog* eventually evolved into the *Whole Earth ‘Lectronic Link* (Well) virtual community.

Secondly, they both served the countercultural desire to create a heterotopian community removed from bourgeois structures and capitalist modes of production. The protocological control in decentralized networks is transferable to the countercultural idea of changing perception in order to change practice in that both technologies struggled to be understood as a means towards that end and not as the end itself. Castells critically acknowledges the risk of losing the ability to communicate face to face through digital media (2009) for context to be lost and communication to become mere signals in a network. This argument can be translated onto debates about controlled substances when consumption becomes an end rather than a means.

Turner (2006) sees both factors – reappropriation of technology and the search for a heterotopia – as central points of the US counterculture. This attitude allowed for some technologies to be combined very successfully. Some of these technologies were reappropriated from a military-industrial complex and fitted a countercultural agenda of decentralization and free-flowing energies. Combination in this context means that the mentioned technologies – synthesized psychedelics and networked computers – were seen by pioneers in the development of home computers and Internet services like Brand and Steve Jobs as fitting countercultural attempts to create a heterotopia through technologies such as psychedelics, music and gatherings (Turner 2006).

To quickly return to Brand's quote, another aspect that computers and drugs share is their potential for recreational use. The counterculture offered a convenient label of political activism to be put on both. What hacktivism also borrows from the counterculture is, in broad terms, a sense of identity. This identity was shaped by an individualistic, romantic hedonism and inspired

> a new cultural toolkit [that] was made available to and rendered compelling within the world of computing [...] it offered a new social meaning for computer use, a new vision of what it meant to sit down at a computer console and of who the person was who was using it – a new idea of self association with computers. (Streeter 2011, 68)

This can also be applied to computer culture and hacking in general, in that a new idea of self-association could be merged with romantic narratives of outcasts and rebellion. To be more specific about how the counterculture helped to shaped hacktivist identity, it is necessary to look at how those cultures embraced outsider roles and very much defined themselves in romantic terms of inside (those who get it) and outside (the man, the state, the square). Streeter relates this to shared experiences:

> When a marginal social movement accurately anticipates in the public eye a significant historical failure of judgment on the part of leadership, the effects can be powerful. Being right about something when the powers that be were wrong, for example, was a central collective experience of the 1960s counterculture; by 1969, the world had watched the television networks, the New York Times, and many members of the political establishment change their position on the Vietnam War. (Streeter 2011, 163)

Counterculture's contribution to a hacktivist identity is thus the "self-association with computers", together with an understanding of those computers to be more than calculating machines, a dichotomy of insider versus outsider (where the hacker of course is the outsider free from the constraints of the system) and a rejection of authoritarian and centralized structures. This countercultural influence can be observed in the Electronic Frontier Foundation’s (EFF) mission statement to “[Protect] Freedom Where Law and Technology Collide” (Electronic Frontier Foundation n.d.).

The countercultural influence on computing is often understood as a clean break from rigidly controlled batch processing towards a flexible and open model of computing. It is thus easily overlooked how much overlap there was between the counter and mainstream culture of the 1960s. The belief that psychoactive substances can be used to improve the overall quality of life may be one concrete example, the strong references to the ideas of an American frontier and the need and right for expansion may be a more abstract one. Reading the novel digital world as a space of continuous expansion, in strong reference to the westward expansion of the American frontier, combines both traditional Western narratives and countercultural ideas of new, openly available space. It was this narrative of what the digital could be that drove many to stake their claim in the digital wild west. Streeter is right in describing the romantic hedonism of the counterculture as based on shared feelings and experiences rather than shared actions (2011, 163). The next section will be focussed on the application of this new and yet old identity. What hacktivism and web defacements take away from the counterculture is a special form of identity: the knowledgeable outsider. This identity will become relevant later on in the discussion of defacer motivation. Nevertheless, the counterculture was not primarily a computer culture so, its contribution to the understanding of web defacements is to be more broadly seen in the engagement with the role of technology and enlightenment thinking in society. The more hands-on contribution of how to actually use these new computing machines was to be found in the emerging computer culture of the time.

2.4 Computer Culture

Computer culture is often seen as one of the developments of US-American counterculture of the 1950s and 1960s. Its contribution to the formation of a hacktivist scene in the late 1990s was the application of countercultural ideas of reappropriation onto computing. In a first move, this reappropriation led to a communication network that became more accessible as devices became both more widespread and affordable. This meant that more people were using computers, but it also helped to disseminate computer technology, as can be seen in the development of the *Homebrew Computer Club* (Petrick 2017). What is needed for the activist part of hacktivism certainly is a critical mass of users, a large enough potential audience. Achieving this on a technical level was the result of continuous development of hard- and software, but on a cultural level depended on the shared understanding of computing as a medium of meaningful expression

Underlying this notion of a meaningful expression coming from a computer is a change in understanding about what a computer is and what it can do. This shift from the computer being understood as an information processor to being a device for symbol manipulation is attributed to Norbert Wiener’s 1948 theory of cybernetics, in which he describes

> automata effectively coupled to the external world, not merely by their energy flow, their metabolism, but also by a flow of impressions, of incoming messages, and of the actions of outgoing messages. (2007, 42)

Wiener’s concept here describes the re-ordering of human-machine interaction. This new understanding would become central to concepts of what computers were and what they could be used for. As machines became more capable, the concept was further developed in Joseph Licklider’s work on Human-Computer Symbiosys:

> [Problems] would be easier to solve, and they could be solved faster, through an intuitively guided trial-and-error procedure in which the computer cooperated, turning up flaws in the reasoning or revealing unexpected turns in the solution. Other problems simply cannot be formulated without computing-machine aid. Poincare anticipated the frustration of an important group of would-be computer users when he said, "The question is not, 'What is the answer?' The question is, 'What is the question?'" One of the main aims of man-computer symbiosis is to bring the computing machine effectively into the formulative parts of technical problems. (1960, chap. 2)

What Licklider does here is lay the foundation for computer culture not as a culture of information processing, but as a culture of computer interaction. Moving the need for a computer to be able to give answers in the background gave rise to a way of interacting with computers for the sake of interaction. This opened up the computing scene and attracted new users that were less drawn towards solving equations but to exploring new possibilities of symbol manipulation.

Engagement took many different forms, and what followed then was a debate about how and if established concepts of law should be translated onto this new communication network of interconnected computers. It was the persona of the hacker as an advocate of this new world who emerged as a result of this debate:

> They [hackers] were appealing because they were presented as the values of a community struggling with and acting on their internal passions, their shared fascinations with tinkering with computers as an end of its own. (Streeter 2011, 90)

Hacking thus is seen as computer culture’s engagement with itself. Computer culture brought about rules and roles for engagement with computers and explored their possibilities by engaging with them. The defining politics during this phase are described as a duality between establishing and disseminating the new identity brought about by new machines and new ways of using them (see Nelson 1983; Naughton 2001), and on the other side a drive to separate this new sphere from established legislation and influence (Barlow 1996).

The early hacking scene was built upon the idea of computing as an end rather than a means towards a goal and helped build the notion that a new space for human exploration and activity had been opened up.

> Across a whole range of information and computer-networked contexts there emerged the sense of there being a 'there' on the internet accompanied by a politics of the 'there'. (Jordan 2015, 184)

This there describes the notion of the web as a separate space. This idea still held true when hacktivism began to gain public attention in the late 1990s. With increasing digitization of everyday life, the there and here have become interwoven. As will be shown in more detail, one of hacktivism's characteristics is exactly this play on the physicality of the digital.

The focus on "there" – on politics specific to computers and computer networks – marks a turn away from the materiality of computers (as sophisticated electronic circuits) towards the virtuality of computers (as a new layer through which to perceive reality). This is similar to Brand's quote about computers and psychedelics from the previous section and my interpretation of it; the moment computer systems were understood as the latest technology through which humankind would expand its consciousness, was the moment where engagement with computers became not a necessary evil but a meaningful and rewarding step towards the betterment of society. Seeing the web as a separate space of course opened the door for the user to conveniently do almost anything and label it politically important within its own reference system.

The addition of computer culture to hacktivism lies in the culture aspect; in seeing computer systems as potentially world-changing systems which need to be supported by an appropriate culture to preserve and enhance their effect. Undertaking this cultural work would be the pioneers who happened to be involved in this early computer culture – hackers, developers, scientists and all early adopters. This is often not adequately described in literature, rather computer culture itself is at times taken as a starting point for analysis, omitting an analysis of the processes which led to its formation. Thus, we must critically analyse the departing point of this culture to understand that the structural conditions which enabled these pioneers were shaped by larger societal structures and that this "new" space was by no means a blank slate.

In reality, the machines of the early computer culture did not offer easy access by any contemporary understanding. They required at least some level of technical expertise, an adequate amount of disposable income, as well as space and time to fit a computer into one's life. That alone should raise suspicion that the computer culture that grew out of the counterculture was anything but ideologically pure. If this point is not adequately addressed, any analysis is at risk of confusing the structure of the early web – such as distributed Usenet forums – with the ideology found in it – usually described as liberal/progressive. This ideological blind spot becomes even more visible when we look at the open source movement and its contribution to hacktivism.

2.5 Open Source

Open source is to be discussed here not as one type of licence amongst others, but as an ideological response to some of the debates around computer and network usage. This response maintains the belief that a software's code (the source) should be freely accessible to all for purposes of learning and improvement.[10] It has been shown that debates about the extension of intellectual property rights from physical onto virtual goods can be read as debates about the commercialization of the web which is often equated with proprietary, so-called closed source software (Musiani 2011).

The years 1991, 1993 and 1994 saw a range of changes that contributed to the commercialization of the Internet, such as the integration of existing business networks (National Science Foundation 2003) and the release of Mosaic, the first graphical web browser. (Holwerda 2000) While both helped to bring more users online, it intensified the need for politics to define how the new medium should be used. The open source movement during this time was an attempt to put cyberutopian ideas into practice and to prevent the web from being taken over by commercial interests.

Open source was as much a way of developing software and managing distribution as it was an attempt to move towards a digital culture of sharing, free access to resources and cooperation as expressed by Howard Rheingold (2000b; 2000a). But open source was not limited to the digital realm. Rather it was seen by some of its key figures as something that came out of software development but should eventually be applied to all modes of production (Stallman and Gay 2002; Raymond 2001). This moment of transferring ideas from hobbyist or side project software production onto a larger economical scale gives another hint as to how the structure of this open source model with its hyper-flexibility, fragmentation of work into projects and workers into skills, together with a dismissal of both governmental regulation and established corporations was shaped by emerging neoliberal ideas.

[10] Emblematic for open source ideals, the “four essential freedoms” for software and users are:

> The freedom to run the program as you wish, for any purpose […] The freedom to study how the program works, and change it so it does your computing as you wish [...] Access to the source code is a precondition for this. The freedom to redistribute copies so you can help others […] The freedom to distribute copies of your modified versions to others [...] By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this. (Free Software Foundation 2021)

The concept of four essential freedoms dates back to Franklin D. Roosevelt's 1941 State of the Union Address (his freedoms being freedom of speech, freedom of worship, freedom from want, freedom from fear) (1941). The use of the concept for open source computing is yet another nod to the political orientation of open source as an ideology.

Following on in this tradition, it is not surprising that open source software and licences are often described with references to computer and counterculture:

> the “free and open-source software” and “free culture” movements have created new institutions to foster collaboration and share information. Free software projects such as Linux (an operating system) and Apache (a web server) bring together programmers who share expertise, resources, and code.
>
> The “geeks” participating in these projects follow what anthropologist Gabriella Coleman calls the “hacker ethic” — an evolving, and sometimes contradictory, set of principles that include, but are not limited to, information sharing, decentralized collaborative governance, distrust of authority, and an understanding of programming as an art form. (Davies and Razlogova 2013, 7)

This “hacker ethic” and “understanding of programming as an art form” echoes earlier notions of identity expressed by countercultural computer pioneers who explored the possibilities of unconnected computers. Just like their countercultural predecessors, open source enthusiasts found themselves in a similar conflict between “distrust of authority” and following a set of principles in the form of a hacker ethic. Open source enthusiasts also lacked a critique of their tools as much as the counterculture did. If we acknowledge that psychedelics may not lead all to Eleusis[11] but some to psychosis and addiction, we must look at a flexible, decentralized type of software production equally critical. The kinds of distributed, often voluntary, forms of work associated with open source production maps onto the dynamics of work associated today with the gig economy. This gig economy is characterized by the remote provision of digital labour through platforms or apps and has been described as increasing flexibility in development, alienating workers and undermining labour regulations (Coyle 2017; Graham, Hjorth, and Lehdonvirta 2017; Vallas 2019). Pekka Himanen describes a new work ethic underlying this mode of production:

> We have seen the seven dominant values of the network society and protestant work ethic are money, work, optimality, flexibility, stability, determinacy, and result accountability.
> The first guiding value on hacker life is passion [followed by] freedom [...] social worth [...] openness [...] activity [...] caring […] (Himanen 2001, 139)

What this work ethic lacks though is a critique of the modes of production that may have led to a certain group of information professionals feeling driven by these entrepreneurial principles. In other words, Himanen’s hacker is oblivious to the origins of his guiding values, he assumes they originate within his self and are merely enacted through his machines. Critique of the physicality of these machines and the historical conditions which led to their widespread adaptation suggests that this is the inverse of how this relationship actually functions.

The hacker ethic described above by Coleman and Himanen shows the translation of neoliberalist ideas – Himanen even recursing to the protestant work ethic – onto hacking. Read in this light, the hacker ethic is little more than an enthusiastic

[11] The Eleusian Mysteries were religious rites in ancient Greece. They have been described as the archetypical psychedelic experience (Wasson, Hofmann, and Ruck 2008).

translation of neoliberal principles onto computing, software development and ultimately hacking. This is an important ideological blind spot to be observed throughout the project. For example, many of the cybercrime archives discussed in this study are built around the quantity of defaced pages above anything and many defacers find themselves struggling with how to formulate a critique of neoliberalism from within this work and hack ethic.

What open source licences and ideology contributed to the formation of a hacktivist identity is twofold. First, it is a revised understanding of authorship. As software projects are complex and build upon previous work, authorship cannot be attributed to a single individual. This process itself is not new and can be found in any larger object produced – for example buildings – as well as in encyclopedic works, but the relative autonomy contributors have in designing software introduces a new sense of autonomy while at the same time lowered the threshold for contributions. Now almost everyone with some programming knowledge could participate in this collaborative effort. This blurring of lines between the user and developer was in sharp contrast to closed-source, proprietary software.

The second contribution is a reaction to copyright debates on virtual goods. Streeter sees open source as a protest against the commodification of data and describes it as one of the few digital traditions that opposed the market:

> What was historically unique about the work of the network pioneers of the 1970s and 1980s is not that they cooperated or worked outside of proprietary formats but that that particular set of extracapitalist procedures appeared in the heart of an emerging high-technology sector in the absence of a military emergency, associated with various countercultural allures, and at a time when American public discourse was aggressively moving towards a universalizing promarket discourse. (2011, 184–85)

The open source movement can thus be described as the attempt by a group of software developers to counter the development of software monopolies they believed to be outdated and counterproductive. Its aim was to disrupt the market, not abolish it. The contribution of open source to hacktivism lies in lowering the threshold for participation thereby enabling an even greater number of people to participate. In this sense, open source helped to mobilize many new users that had just come online. This new sense of what it meant to participate on the web also was amplified by a shared understanding that data was not a commodity but should be freely available and protected from monopolization through licences.

Complicating the ideas of the open source movement is its often overlooked entanglement in economic and social structures, much like in the case of the computer culture. This means that while Free and Open Source Software (FOSS) is made available free of charge, it depends on material goods (hardware) and labour (software). Richard Stallman (2009) coined the expression that free in the context of FOSS should be understood as in “free speech” and not as in “free beer". Expanding from the open source movement to the idea of digital commons[12] brings questions of access and usage rights to the fore. Writing in 2010 on Indymedia, Scott Uzelman argues:

> Against those formulations that present the commons as resources available to a public without limits, I argue that commons should be understood as limited, community-managed resources founded upon crucial and constitutive exclusions. (2011, 280)

For Uzelman, digital commons are born out of a community managing their limited resources in relation to an outside. This necessitates a group identity and self regulation. The scarcity of resources can be dictated by outside forces (persecution of hacktivists) or by the medium itself (limited attention). This materialist perspective is shared by Johann Söderberg in his 2008 work *Hacking Capitalism: The Free and Open Source Software Movement:*

> machinery is designed with three purposes in mind: to direct work tasks, to evaluate the performance of workers, and to reward and discipline them. [...] The fact that a technology rarely fulfills the expectations of its inventors does not rule out the existence of an agenda behind designing the technology in a particular way. The reason that a design falls short of regulating the behavior of users is because the users are opposing the agenda. (2008, 89)

This implies that the scarcity of resources in the digital is not a temporary condition to be overcome by better machines; it is a defining factor for the whole world of human interaction. Further, Söderberg acknowledges that subversion (hacking) is the reaction to a flawed design. These ideas are also to be found in the 2008 *Copy, rip, burn: the politics of copyleft and open source* by David Berry:

> early experiences by programmers and developers tended to reinforce the notion that software was a public "informational" good that should be freely shared, and indeed the concept of property or ownership of software was an anathema to the ethics of the early hackers who proved their skills precisely by *showing* [emphasis in original] and sharing how cleverly they could program. […] This operating system [Unix] used a clever way of sharing the computer processing time amongst a number of users, as a single processor was such an expensive piece of hardware. This early experience indoctrinated the early programmers with the principle of sharing resources amongst themselves – the "commons" was understood as the amount of processor time and software that was available that had to be shared equitably between different users. (2008, 106–7)

Both authors clearly disagree with the idea of inexhaustible digital commons. The community Berry describes here is not based on abundance, but on scarcity of both hardware and time and consequently ensured that the distribution of these was of consequence. Note that Berry uses the expression "indoctrinated" here to describe how early computing infrastructure shaped parts of the hacktivist community. Their idea of free information and unrestricted access was for Berry

[12] The "Tragedy of the Commons" is a concept introduced by the economist William Foster Lloyd. (1833) While used by Lloyd to describe regulation of common lands, his concept is often used when talking about what constitutes digital resources and their usage. The essential argument is that digital commons require ongoing labour to be maintained, while they also need to be protected against commercial exploitation.

not a conscious decision, not the effect of countercultural influence but the effect of what Söderberg would call machinery (2008, 89). This understanding of a digital community shaped by the infrastructure around them is most prominently expressed in the works of Alexander Galloway's and Eugene Thacker's 2006 *Protocol: how control exists after decentralization.* The authors develop a critique of control and agency in distributed networks that counters the idea of technophile liberation through being part of the network:

> Protocol [the rules for information exchange] does not produce or causally affect objects, but rather is a structuring agent that appears as the result of a set of object dispositions. [...] Protocol is always a second-order process; it governs the architecture of the architecture of objects. Protocol is how control exists after distribution achieves hegemony as a formal diagram. It is etiquette for autonomous agents. (2006, 75)

This view sees users not as creators, but as products of the same tools they are allowed to employ to a limited degree. Galloway and Thacker's post-humanist theory is very useful to see beyond the narratives of individual agency in the open source movement and WikiLeaks as it places increased agency on the side of the network of machines and the regulations governing the exchange of information between these machines. In the context of hacking and hacktivism, the engagement with protocol as described by Galloway and Thacker has its roots in offline activist's culture jamming to disrupt the normal flow of information and the normal function of space.

What the discussion of web defacements takes away from this section on open source is the acknowledgement that a critique of the tools used in hacktivst defacements – from computers to hacking practices to defacement archives – is yet to be written. This gap in research is an important finding and leads into the next section which investigates the often makeshift critical engagement with computers and software as objects of pure reason made by hackers and hacktivists.

2.6 Culture Jamming

If the open source movement and computer/hacking culture helped create a sense of identity and purpose for online activities, the question still remains as to what motivation users might have had to engage in hacktivism. Open source in the context of hacktivism must be understood as an ideology that promotes access to the means of digital production while culture jamming is a set of practices for hacktivists that does not carry any inherent ideology. Culture jamming is defined as

> a genre which critiques popular/mainstream culture, particularly corporate capitalism, commercialism, and consumerism. Here, media artists and activists appropriate and 'repurpose' elements from popular culture to make new works with an ironic or subversive point. (Lievrouw 2011, 22)

It must be acknowledged how the toolkit provided by the Situationists and the postmodernist left has contributed to the practices nowadays known as hacktivism. The most fundamental definition of the relationship between mass media and critical practice was provided to the countercultural scene in 1967 by Guy Debord:

> The widespread use of receivers of the spectacular message enables the individual to fill his isolation with the dominant images – images which derive their power precisely from this isolation. […] Critical theory must be communicated in its own language. It is the language of contradiction, which must be dialectical in form as it is in content. It is critique of the totality and historical critique. It is not "the nadir of writing" but its inversion. It is not a negation of style, but the style of negation. (1994, secs 172, 204)

This “style of negation” is exactly what is central to culture jamming when used in the context of hacktivism. It can take on basic forms such as disabling digital infrastructure with the intention to interrupt the spectacle momentarily. More advanced forms of culture jamming include trolling – intentionally sabotaging a discourse to reveal its hidden agenda – or take the form of rapidly spreading memes that subvert established symbolic links.

A practical application of the connection between the Situationists and culture jamming is described as a shock therapy:

> Interrupting the stupefyingly comfortable patterns we've fallen into isn't pleasant or easy. It's like crawling out of your warm bed in your dark room one December morning at five A.M. and plunging into a tub of ice water. It shocks the system. But sometimes shock is what a system needs. It's certainly what our bloated, self-absorbed consumer culture needs. (Lasn 2000, 107)

Lasn is focussed on adbusting – the subversive reappropriation of advertisements – but also refers to new ways of culture jamming provided through the Internet:

> The Internet is one of the most potent meme-replicating mediums ever invented. [...] Cyberjamming is evolving at a dizzying pace. Here are a few interesting techniques in use at the time of this writing: Cyberpetitions [...] Virtual Protests [...] Virtual Sit-ins: Immobilize an enemy site by organizing a few dozen cyberjammers simultaneously to request more texts, pictures, animations and multimedia elements than the site can handle. [...] Gripe Sites: Create and maintain a site dedicated to uncooling one particular corporation or brand. (Lasn 2000, 133)

From the previous discussion of counterculture and mainstream influences, it could be assumed that hacking and hacktivism is inherently liberal-progressive in orientation.[13] However, hacktivism has been politically diverse from the start (Samuel 2014), contradicting the prominent narrative of it being inherently liberal:

> Just a few years ago the left-cyberutopians claimed that ‘the disgust had become a network’ and that establishment old media could no longer control politics, that the new public sphere was going to be based on leaderless user-generated social media. This network has indeed arrived, but it has helped to take the right, not the left, to

[13] Outside the scope of this study, computer industries and user groups also existed in socialist countries. For an introduction, see Goodman (1979) Erdogan (2020).

> power. Those on the left who fetishized the spontaneous leaderless Internet-centric network, declaring all other forms of doing politics old hat, failed to realize that the leaderless form actually told us little about the philosophical, moral or conceptual content of the movements involved. Into the vacuum of ‘leaderlessness’ almost anything could appear. (Nagle 2017, 27)

Nagle here is very clear about the distinction between forms of organization and political content. This assumed automatic overlap of political content with technical infrastructure can be seen in many studies of Internet political cultures (Matic 2004; Lingel 2017; Calhoun 2004; Dahlgren 2013). However, rather than assume correspondence between form and content, it is important to observe the articulations coming from those systems and the processes they entail. This again highlights the necessity of a critique of tools. Going back to hacktivism, this means that any instance must be framed within existing power structures and must be thoroughly critiqued as a tool. An example of this can be found in the emerging debates about the integration of cyberattacks into the military arsenal, as seen in the case of the Stuxnet virus, a program apparently designed to target the Iranian nuclear program (Kerr, Theohary, and Rollins 2010).

The borders between hacking, culture jamming and trolling are fluid. This is exemplified in the practice of manipulating the Bell phone network. What started as a mix between hacking, exploring and exploiting the network to make free calls (Lapsley and Wozniak 2013) eventually grew into one prankster spreading false information about a nuclear explosion in Santa Barbara (Coleman 2014). Culture jamming methods were easily adapted to the early web, especially because it was more fragmented than the platformized Internet of 2019, having less distinction between user and creator. Also, the technology was simply more prone to breaking on its own (a kind of automated culture jamming) and easier to break. A steady decline in the number of web defacements (Balduzzi et al. 2018) shows that online security is increasing to the point where even private websites are not automatically easy targets anymore.

It was mentioned before that the various strains of countercultural theory and practice had as a common denominator a critique of pure rationality expressed through technocracy and how hacktivism and web defacements can be seen as the application of said critique. What this section of culture jamming adds to the understanding of web defacements is that it reveals yet another theoretical underpinning of web defacements. As an applied critique of technocracy, defacements are more than nuisances, they are translations of earlier practices of culture jamming, detournement and critical theory. What made the application of said practices onto the digital sphere special and worthy of a close investigation is that they happened in a narrative-laden space.

2.7 Cyberspace

During the attempt to explain the ideological roots of hacktivism, the objects of study have shifted from actual technologies such as home computers and computer networks to ideologies such as open source and even practices like culture jamming. This is since these are configured according to a narrative of how they should function. Hackers, including web defacers, do not merely use technologies that make up the Internet, they change and shape that medium through their interaction. As defacers help create archives of their work, they not only create new stories through their work, the archived material itself becomes a story. Streeter relates this form of engagement with technology to a romantic response to technology as such:

> The Weberian narrative of disenchantment with the modern [...] provides a compelling general sense of the draw of romantic postures and narratives; in Weber's terms, faced with life in the iron cage of modernity, we despair at the lack of enchantment and seek for ways to bring it back.
>
> First, it needs to be said that in many cases, it was not digital technology itself that transmitted romantic ideas. Romantic tropes, in fact, were largely picked up in printed texts. [...]
>
> Second, computer countercultural romanticism had a specific history, a cultural context. John Perry Barlow, Ted Nelson, and Stewart Brand had read and created reams of 1960s countercultural literature, as had many of their readers. [...]
>
> Third, romanticism was reactive. Romanticism should not be overgeneralized to the spirit of the times in the Hegelian sense, an essence that permeated all aspects of society and culture. It made sense only if it had something to be against, something with which it could be contrasted. In the case of computer counterculture, it gained traction as a response to other specific modes of thought and their contradictions. (2011, 170)

If the previous parts of this chapter attempted to explain why hacktivism grew to popularity when it did, Streeter here helps to understand the choice of medium. According to him, it is not that romantic tropes were invented on the web, but it was here that they were readily adapted. The need to contrast romanticism against “other specific modes of thought” helped to create a need for the underdog, fighting-back-from-the-margins self-understanding of 1990s hacktivism. The concept of cyberspace provided the base from which this understanding could operate as it embodies much of the romantic tropes of the early Internet. Contrasting the term “cyberspace” with expressions such as “information superhighway” shows that the first echoes with romantic themes of manifest destiny and frontier expansion while the second shows an understanding of the web as yet another piece of infrastructure made to deliver information much like physical highways help deliver goods and people but usually do not allow for new forms of expression and identity. Cyberspace was the expression of the web as a place with separate identities and politics:

> amid the widespread articulation of the new networked realm as a place, most often then called cyberspace, there emerged a political conception of what this place should be. In varying places and varying ways, some of which, like Levy’s articulation of the Hacker Ethic, became world famous and others of which sank without a trace, there were attempts to develop the idea that social and cultural

> activity on global computer networks formed not just a new place or land but a place or land with a particular and innate kind of politics. (Jordan and Taylor 2004, 178)

This understanding of the web as a place with innate liberal and progressive politics is a key factor in understanding why participatory culture was so important on the Internet of the 1990s and also why it was designed to emphasize participation.

Contrary to the belief that hackers would remain the keepers of cyberspace, but in line with reading cyberspace as a novel space for human interaction (and legal regulation) is Lawrence Lessig's emphasis on the design of cyberspace as a regulator:

> This regulator is what I call "code"—the instructions embedded in the software or hardware that makes cyberspace what it is. [...] And if in the middle of the nineteenth century the threat to liberty was norms, and at the start of the twentieth it was state power, and during much of the middle twentieth it was the market, then my argument is that we must come to understand how in the twenty-first century it is a different regulator—code—that should be our current concern. (2006, 121)

Lessig makes clear that cyberspace itself does not contain ideology, but that it is shaped by the conditions (hard- and software) that constitute it. Following from this, no hacker ethics are natural to it, but are just one form of hegemony that will eventually be replaced by more powerful corporate and state influence.

Cyberspace as a new space for human interaction would become attractive for commercialization as soon as enough users were online. This new frontier would then be settled and user roles which burred creator/designer and consumer would be redefined. Nevertheless, the idea that hackers are inherently liberal and progressive persists. As this and the previous sections have shown, the question of hacker and defacer ideology is more complex than that. What this section adds to the discussion of web defacements is the acknowledgement of cyberspace as a powerful narrative of the web as a place with separate identities and politics. This narrative, problematic as it is, continues to shape and obfuscate the understanding of the Internet.

2.8 Web 2.0

The defining moment for hacktivism to evolve from a fringe phenomenon towards political and social mainstream was the introduction of Web 2.0, a move away from the static homepage to dynamic user-generated content delivered through platforms such as emerging social media. This development lowered barriers of entry even more than the introduction of the World Wide Web, but brought with it a clear push towards the user engaging with content in clearly defined ways - a step away from the DIY-culture of the early web. Further, those platforms were designed to be commercially viable walled gardens rather than homesteads on the wild web (Chandler and Munday 2016; Higa 2008). Its consequences for the development of hacktivism were twofold.

Firstly, social media allowed for publics to form in ways that were more fluid than the previous static content allowed for. These publics tend to form over topics which caused strong emotions, hence they are described as “affective publics” by Zizi Papacharissi (2016). These affective publics are ideally suited for interventionist action using graphic content, while at the same time allowed easy organization of collectives. To reach these new, affective audiences, Nagle argues that a Gramscian turn from politics towards culture took place:

> They [the alt-light] were the youthful bridge between the alt-right and mainstream Trumpism. Although the tactics of the online right are updated to a digital age, it is hard to think of a better term than Gramscian to describe what they have strategically achieved, as a movement almost entirely based on influencing culture and shifting the overton window through media and culture, not just formal politics. (2017, 41)

This alt-light politicised online culture, represented a return of an interest in politics within some online communities. Looking at hacking cultures, it is striking how much in their agendas and manifestos were concerned with creating a digital locus amoenus, far away from the disappointments of real-world politics (Curtis 2016). If the alt-light is to be seen in a larger hacktivist context, it symbolizes a politicized online culture adapting to a platformized web used by enough users to exert large influence.

Secondly, this new way of interacting with an (involuntary) audience required new tactics. To be more precise, it required a total reconfiguration of tactics. Hacktivism in the context of a platformized web means to engage with the platform to influence the formation of affective publics and the nature of debate. Rather than obtaining control over a platform’s server, hacktivism on the web 2.0 seeks to obtain control over the platform’s content (Trottier and Fuchs 2014). That is not to say that breaking into systems has become obsolete, but rather that hacktivism during this phase is closer to the psychedelic “changed practice through changed perception” approach of the counterculture.

These new platforms also brought about an atomization of strategy. Instead of big hacks done by a select elite, collectives such as Anonymous emphasized many small contributions by a large collective to achieve operational success. This may be seen in Anonymous’ Low Orbit Ion Cannon (LOIC), a denial-of-service attack software that relies on a voluntary botnet, meaning that many users have to run the software at the same time to achieve an effect (Deseriis 2017).

The guiding politics of this phase are subsequently centred around control of social media platforms, be it through questions of copyright violations, privacy issues or content labelled hate speech.

Daniel Trottier and Christian Fuchs in 2015 claim that social media’s emphasis on cognition, communication and cooperation were vital for the formation of online identities that would translate into on- and offline activism (cf. S. Salem 2014). It is worth noting that with the shift towards social media, technical aspects seem to become less important: the mobilization and control of communication commons (social media) is more important than technical expertise (Fuchs 2014). Other authors, looking at the 2011 Egyptian revolution and efforts of state censorship, seem to agree with this notion of content over technology. Sarah Salem attributes the roots of the formation of social media activism during the Egyptian revolution to the availability of satellite TV (2014), while Thomas Poell agrees with the notion that social media can be a tool for the formation and mobilization of hacktivist activity (2014).[14]

This shift in focus came with an incorporation of new theories from communication studies. The works of Manuel Castells in particular have had great influence on broadened definitions of hacktivism. In his 1996 work *Rise of the Network Society*, the thought of a global society defined by electronic means of communication was developed, building on previous work (Castells 2010; McLuhan 1962; Rheingold 2002). His subsequent work *Communication Power* expresses the central role of influencing communication systems. Castells states that "power relies on the control of communication, as counterpower depends on breaking through such control" (2013, 3). In this context, hacktivism is part of the counterpower attempting to affect communication as much as possible. Although hacktivism is not the central theme in Castell's works, the theory developed here frames hacktivism as a core concept in this struggle over communication power. Castells mentions hacktivism's potential to disrupt politics and to be used as a corrective: "the subjects can now watch the powerful, at least to a greater extent than in the past" (2013, 413).

Looking at a case of hacktivism which has undoubtedly had great influence on politics – WikiLeaks – is the 2013 work of Bart Cammaerts *Networked Resistance: The Case of WikiLeaks.* In it, the author frames WikiLeaks within broader debates about online activism and media theory:

> the case of WikiLeaks should be positioned within a broader legacy of information and communication activism and more specifically related to newly emerging repertoires of networked contentious action also at times denoted as hacktivism. Hacktivism compounds hacking and activism and as such it represents the extension of sociotechnological struggles into the realm of politics beyond the technological and the networked computer infrastructures. (2013, 421)

Interesting to note here is that Cammaerts sees WikiLeaks as a part of "communication activism", or hacktivism. This confirms the notion of WikiLeaks as part of an activist tradition that has expanded into the digital. While the demand for transparency is shared among many initiatives, "radical freedom of information activists [argue] that legal activism is not enough and [adopt] more radical tactics such as anonymous whistleblowing" (Cammaerts 2013, 425).

[14] That these thoughts on the role of social media have far-reaching consequences can be seen in the work of OONI, a project to measure Internet interference. Their reports show how – beyond individual examples – the restriction of services and connections is a regularly used tool in the context of electoral politics.

Cammaerts (2013) agrees with Samuel that hacktivism is reacting to and interacting with existing structures rather than serving as a creative force.

This section on web 2.0 describes the moment in which hacktivism and defacements broke into the mainstream. With the ever more widespread digitization of life, counter-movements would no longer be translated from the streets onto the web. Rather the web would influence real-world politics. This section’s addition to the understanding of hacktivism and defacements is the acknowledgement (again, the under-researched acknowledgement) of the pivotal role web defacements may play: they are a bi-directional gateway between the streets and the web.

The previous sections outlined the lineage of web defacements. They did so by drawing from various traditions, movements and schools of thought and remained largely abstract, referring to defacements as concepts. This was necessary to sketch out the theoretical underpinnings of web defacements and to identify blind spots in research. Still, what is needed is more understanding of what defacers and hacktivists actually do. The remaining sections in this chapter will now turn towards the more concrete aspect of defacements.

2.9 Storage and Digital Memory

Moving on from the theoretical lineage of hacktivism and web defacements, the following two sections are going to outline the effects and usage of web defacements. These effects are to challenge/alter news frames within the public debate, and thus intervene in public memory making, and to compete for or even hijack attention. Defacers do so by making use of the machine-dependency of electronic media which offers a multitude of ways to interfere with the facilitating infrastructure.

The first and most obvious way hackers intervene in memory is by over-writing existing stories and creating new public stories. Secondly, hackers also intervene in public memory by archiving their activity. The so-created archives are themselves an intervention into memory. These are the connecting points between hacking, storage and memory.

To understand why defacers would engage in such practices, it is important to understand their actions in relation to the current state of information technology. The aforementioned romanticism of the web has two important aspects to it which are helpful here. One, it reacts to increasing technologization of life by referring to the technical history of the past. A common critique of the web 2.0, for example, hardly calls for abandoning the web altogether but values web 1.0 as more creative, permissive, and the like. This is done by creating a narrative of what the past used to be. Second, it is not a Luddite movement but a vision of how technology can be used in the future. Hacking, free and open source software and digital commons all can be understood as critiques of the management of technologies rather than critiques of technology itself. It is this factor that ties hacktivism so closely to existing power structures. It is also this factor that distinguishes hacktivists from digital vandals or terrorists: hacktivists engage with technology, sometimes in destructive and illicit ways, and in doing so critique the application, content and role of this technology in society. However, they do not hack to destroy the technology, but rather to reclaim it. This important distinction is grounded in the previously discussed romanticism of the web and the open source-inspired ideal of technology as a public good. By intervening into the flow of information through the additional layers and interfaces of digital media, defacers are intervening in public memory.

These additional layers and interfaces demand special consideration, as they are one of the key factors describing the relation between hacktivism and media. To approach this concept, consider how archived web material is both born-digital content as well as content mediated through electronic devices. It is, to follow Niels Brügger, "reborn digital media". This dual role stems from the dual nature of web content, in that it is at the same time a machine-readable information and human-readable mediated content (Brügger 2018). This approach connects the user experience – the way content is mediated through a device – with the content itself. It also opens up new ways of engaging with the content, since it is constituted by both hard- and software (Kirschenbaum 2012).

To further understand the effects of hacking, memory and storage on society, the first task is to critically describe their interconnection. Blom et al. in their 2016 work *Rethinking Social Memory: Archives, Technology, and the Social* argue that a Barthesian second-order process governs the relation between content and infrastructure:

> [There is] ambivalence of the promise of storage. With digital technologies, nothing is stored but code: the mere potential for generating an image of a certain material composite again and again by means of numerical constellations. (Blom, Lundemo, and Røssaak 2017, 12)

Wolfgang Ernst and Jussi Parikka agree with this notion of code-dependency: Following in this lineage of postmodern understanding of the archive and its functions is the field of media archaeology as described by *Digital Memory and the Archive* (2013) which describes media archaeology as "modes of writing that are not human products but rather expressions of the machines themselves, functions of their very mediatic logic" (2013, 12).

This thought is also found in the 2009 work by Andrew Hoshkins who states:

> contemporary memory is thoroughly interpenetrated by a technological unconscious in that there occurs a "co-evolution" of memory and technology. Memory is readily and dynamically configured through our digital practices and the connectivity of digital networks. (2009, 91)

This means that for any defacer activity – archived or live – we have to consider that the content is very closely connected with the infrastructure of the archive and the infrastructure of the user. This mirrors early postmodern thought on the effects of digital media such as expressed 1967 by Guy Debord:

> a tendency to make one see the world by means of various specialized mediations (it can no longer be grasped directly), naturally finds vision to be the privileged human sense which the sense of touch was for other epochs; the most abstract, the most mystifiable sense corresponds to the generalized abstraction of present-day society (1994, sec. 18)

and 1995 by Jacques Derrida and Ernst Prenowitz in *Archive Fever*:

> the technical structure of the archiving archive also determines the structure of the archivable content even in its very coming into existence and in its relationship to the future. The archivization produces as much as it records the event. This is also our political experience of the so-called news media. (1996, 10)

Note that earlier Derrida and Debord both mention mediation either as taking place through archiving or through “various specialized mediations”. In doing so, they hint at their understanding of the archive as one part in a larger assembly of cultural memory. The archive, the repository or the memorial can become sites of memory if incorporated into a cultural process. Astrid Erl and Ann Rigney describe this process of mediation in their 2009 section of *Mediation, Remediation, and the Dynamics of Cultural Memory:* “[Memory] is as much a matter of acting out a relationship to the past from a particular point in the present as it is a matter of preserving and retrieving earlier stories” (2009, 2).

This notion of retrieving something is the connecting point between the archive and the memory site. The archive can become a site of memory and as such may be altered itself:

> canonical “memory sites” themselves have a history and, although they represent in many ways the terminus ad quem of repeated acts of remembrance, they only continue to operate as such as long as people continue to re-invest in them […] they may be replaced or “over-written” by new stories that speak more directly to latterday concerns […] (Erll and Rigney 2009, 2)

When I use the term digital memory rather than archive, I do so because memory is different from archives. While memory can share characteristics and while an archive can be (part) of a space of memory, archives rely less on participation and engagement than other spaces.

Hacktivism’s contribution to shaping this memory is in engaging with both sides of the hard- and software duality. It allows tranforming any website into an unexpected encounter with past events (such as defacing a site for political purposes) and at the same time to engage in a global circulation of information from which understandings of the past are derived. This “intersection of journalism and democratic participation” (Dahlgren 2013, 177) allows to insert information into a discourse, making hacktivism a tool to break into a public sphere.

2.10 Changing the frame

If the previous section was primarily concerned with outlining the structural conditions which enable hacktivism, this section will investigate the communicative function of web defacements. To relate this discussion to the narratives deployed through web defacements, Barthes' concept of myth-making will be adopted, since the process of myth-making is suited for a transposition onto the narrative-generation and information-provision in defacements. In Barthes' work, building on the Saussureian tripartite language model[15], myth is described as a second-order process of meaning:

> In myth, we find again the tri-dimensional pattern which I have just described: the signifier, the signified and the sign. But myth is a peculiar system, in that it is constructed from a semiological chain which existed before it: it is a second-order semiological system. That which is a sign (namely the associative total of a concept and an image) in the first system, becomes a mere signifier in the second. We must here recall that the materials of mythical speech (the language itself, photography, painting, posters, rituals, objects, etc.), however different at the start, are reduced to a pure signifying function as soon as they are caught by myth. Myth sees in them only the same raw material; their unity is that they all come down to the status of a mere language. (2006, 113)

Signs, and that includes material objects, become mere signifiers in Barthes' concept of myth. As soon as they are "caught by myth", they transform into raw material for the second order process. This concept explains why the embedding of objects (in our case, pictures, names and information) in context is important, as this is the process which transforms them from material into memory. It further explains why effort is invested into manipulating or contesting them, since by changing the normative connection between denotation and connotation of the semiological chain the resulting myth can be altered. Objects gain their significance from being embedded in a narrative, such as a defaced page featuring the smoke-covered skyline of New York on the 11th of September 2001, which is not only testament of one event, but are metonymic of the Western world's experience of that day which again is embedded into the context of geopolitical events.

The choice of the word "embedded" hints at the narrative function I assume is had by memory objects such as defaced webpages and hacktivist archives. They function in relation to other objects, forming a relational web where meaning is expressed by the relations between two or more memory objects. The consequences of this approach are twofold: First, these memory objects do not "store" memory within themselves. The General Post Office (GPO) in Dublin, for example, does not exercise any memory-invoking power unless the GPO as a memory object is put into relation to other objects that belong to the sphere of the Irish struggle for independence. Embedded means that memory objects obtain their authority and meaning through the network configuration (such as specific

[15] Referring here to the classic semiotic model of sign, signifier and signified as defined by Saussure (1966).

temporal and geographically defined cultural contexts) they are positioned in. Barthes describes this embedding in the dual function of a press photograph:

> Connotation is not necessarily immediately graspable at the level of the message itself (it is, one could say, at once invisible and active, clear and implicit) but it can already be inferred from certain phenomena which occur at the levels of the production and reception of the message: on the one hand, the press photograph is an object that has been worked on, chosen, composed, constructed, treated according to professional, aesthetic or ideological norms which are so many factors of connotation; while on the other, this same photograph is not only perceived, received, it is read, connected more or less consciously by the public that consumes it to a traditional stock of signs. Since every sign supposes a code, it is this code (of connotation) that one should try to establish. The photographic paradox can then be seen as the coexistence of two messages, the one without a code (the photographic analogue), the other with a code … (1987, 19)

Barthes' description of the dual function of the press photograph aligns with the description of objects as signifiers in a myth-making process. It assumes that the photograph is brought into relation "to a traditional stock of signs", the same way that any memory-invoking object is in relation to a network of social, cultural and local memories. It is this relation which turns an administrative building into a memory site.

Following from this is the assumption that memory objects can change their narrative function if their "embedding" – the web of related surrounding objects – is changed. That this is the case can be seen in many controversial memory objects. Often change in power brings with it a change in the configuration of memory objects, so that their narrative function is changed. This changeability of memory objects, this understanding of their narrative function through their configuration in a meaning-producing relational web, is the entrance for hacktivism. Hacktivism is a practice that is put into action by the belief that the narrative function of memory objects can be changed through the strata that enables them. In the context of digital media, this means the belief that through engaging with the digital media, this relational web of meaning-generating relations can be changed.

This engagement is led by the narrative function I have described earlier: the object itself does not matter as much as its context. Metonymy is the guiding principle for challenging power through activism, to force an association with your own message. To return to the GPO, it is important to note how the Easter Rising (1916) was rather unsuccessful for the Irish cause but hugely influential for Irish history that followed. It is also the guiding principle of terrorism, as the darker side of activism. Modern terrorism is effective by breaking the illusion of control, by forcefully associating the public space with the memory of one public space that was attacked. Its effects are not only the immediate death and destruction but also the long-term changes to the described narrative embedding.

Kevin McDonald in a 2015 article *From Indymedia to Anonymous: rethinking action and identity in digital cultures* contrasts Indymedia (an independent news network born out of the anti-globalist movement) with the hacktivist collective Anonymous. He describes the potential for digital spaces of memory to function even in ephemeral settings:

> 4chan [a forum Anonymous originated from] has had from its beginning a culture of the ephemeral – communication is fragile to the extent that if no one responds to a post, no trace of it remains. The ephemeral nature of posts combined with their anonymity confronts the users of boards with a question of meaning – how does a board create a sense of shared experience, something that extends beyond the brief period that individual posts are present? (2015, 972)

As described by McDonald, spaces of memory are defined by practice. An archive can hold an infinite amount of information, but it is the agency of a human or computational actor which translates the material into memory. McDonald continues:

> Anonymous and Facebook represent two radically different approaches to digital social space, evoking themes developed by Touraine when he proposes that societies are the product of systems of action built up around shared, but contested, core cultural orientations, in this case, practices of memory and selfhood associated with digital communications. (2015, 979)

McDonald talks about “practices of memory” taking place on (or behind the scenes of) two different websites. He further mentions how those practices can be contested but leaves open how this contesting is realized. Hacking and defacing websites can be one way this digital communication can be contested. Through digital communication and “practices of memory” (the archiving of defaced pages in community archives) the online culture of hacktivists expresses itself.

These expressions of community take place in the context of a number of different frameworks. A community of web defacers exists within an attention economy (views per defacement), in a meritocracy (most skilled attacker defaces the most pages) and under latent legal pressure. What this means for the place of this expression of community (the cybercrime archives) is that they can hardly be described as a mere repository, but rather as themselves actors within these frameworks. Attracting visitors, avoiding legal attention and fostering competitive hacking all means that decisions will be taken towards a sustainable business model within the attention economy. Thus, the politics of these archives must be considered. Tarleton Gillespie (2010) criticizes the use of the seemingly neutral term “platform”, yet his critique may be applied to “archive” as well:

> Despite the promises made, ‘platforms’ are more like traditional media than they care to admit. As they seek sustainable business models, as they run up against traditional regulations and spark discussions of new ones, and as they become large and visible enough to draw the attention not just of their users but of the public at large, the pressures mount to strike a different balance between safe and controversial, between socially and financially valuable, between niche and wide appeal. And, as with broadcasting and publishing, their choices about what can appear, how it is organized, how it is monetized, what can be removed and why, and what the technical architecture allows and prohibits, are all real and substantive interventions into the contours of public discourse. They raise both traditional

> dilemmas about free speech and public expression, and some substantially new ones, for which there are few precedents or explanations. (2010, 359)

Gillespie here specifically talks about YouTube, but his criticism extends to all digital media “platforms”. This emphasis on participation is a connecting point between sites of memory created by hacktivism such as WikiLeaks, more traditional archiving and dissemination attempts such as the Internet Archive and profit-driven social media. Gillespie’s focus on platforms seeking sustainable business models through attention converted into revenue shows how important attention is for digital platforms and services. The next section will describe the role of attention as a key resource in the circulation of information.

2.11 Attention economy

The Internet has been famously described as an attention economy where attention translates into interactions which in turn translate into marketable data (Odell 2019; Beller 2006; Tufekci 2013). This is well researched in relation to big platforms – probably the best known work on the topic being Zuboff’s T*he Age of Surveillance Capitalism (2018)* – but the topic leaves questions open when applied to small and potentially subversive actors.

Firstly, web defacers have little to no means of converting attention into revenue the same way platforms do. If their actions are to be described as driven by a desire to be successful in an attention economy, other motivations must be found. These motivations can be divided into motivation related to the message, where attention aids the communication of a message, and motivations relating to their own scene, where attention translates into recognition. This means that while attention does rarely translate into revenue for defacers, attention still holds an important position. The previous quote by Gillespie mentions the dilemma of striking a tone “between niche and wide appeal” (2010, 359). This dilemma between scene-internal and scene-external modes of communication will surface again in the analysis of defacements.

The idea that defacers would be experiencing any sort of dilemma regarding their communication strategy in the first place is indicative of the fact that defacer’s common portrayal as hedonistic individuals roaming the cyberspace cannot be upheld as such individuals simply would have no interest in how their message is perceived. Instead, defacers are active participants in the attention economy, subjects to its laws and conventions. Since defacers deal less in user interaction but in information, an appropriate concept to describe the context of their activities is information capitalism (Streeter 2011; Robins and Webster 1998) where, in the case of web defacers, both technical information on how to hack pages as well as contextual information to be released via these pages function as capital.

Information as capital for defacers does not only include novel information for an educated public to consider. It also, and perhaps most prominently, includes what Castells has termed communication power:

> the battle of images and frames, at the source of the battle for minds and souls, takes place in multimedia communication networks. These networks are programmed by the power relationships embedded within the networks… Therefore, the process of social change requires the reprogramming of the communication networks in terms of their cultural codes and in terms of the implicit social and political values and interests that they convey. It is not an easy task. (Castells 2013, 302)

Defacers' attempts to participate in this reprogramming of social networks shows motivation beyond scene-internal recognition. It has been described by Castells (2010) and Andrejevic (2013) that information abundance leads to a rise of meta-narratives. Defacers, driven by the motivation to be successful actors in this attention economy, are likely to follow this trend. The topic of defacer motivation as a whole is under-researched and will thus be a special focus in the following chapters.

2.12 Conclusion

Reviewing the literature has shown that hacktivism is a complex phenomenon which is positioned within a tradition of critique of technology, re-appropriation of the same and a strong romantic perspective on the past and future. As essential influences on hacktivism, I identify the following cultures, practices and ideologies:

Influence	**Approx. time period**	**Contribution**
Counterculture	1950s-1960s	Disdain for centralized structures and technocracy; re-appropriation of technologies
Computer Culture	1960s-1980s	Shaping the "hacker" identity, dedicated computer and online policy
Open Source	1980s-2000s	Digital commons, copyleft
Culture Jamming	1960s-present	Subvert mainstream narratives and images, reappropriate media
Cyberspace	1980-2000s	Internet as a new and open place for human activity

Table 2.1: Summary of influences on hacktivism and web defacements

These influences stem from a number of intellectual and cultural traditions as mentioned above. Analysis has shown that much of the existing literature does not adequately take into account the ideology contained in those influences. Rather, and I trace this back to early computer culture, structure is equated with content, leading to the false assumption that the web was inherently liberal because of its supposed decentralized structure. What is further missing is a critique of the tools and methods used, such as open source development requiring investments of unpaid work and thus being less open than the name suggests. Ideas of culture jamming add to the frame of dystopian corporate state versus lone hacker rebels. This is most visibly expressed in what I describe as the knowledgeable underdog mentality, the self-ascribed role of an outsider seeing through the mechanics of the mainstream. That defacers are anything but outsiders given their cultural practices are rooted in neoliberal ideology produces a constant conflict. The romanticism of the underdog is powerful, as it motivates people to commit to seemingly insignificant acts by isolated individuals that are believed to add up to significant collective actions – and it occasionally succeeds. The analytical shortfall of equating structure with content can, however, lead to a dangerous simplification of political situations, replacing power with the representation of power. The situation of web defacers is further complicated by the situation in which defacements are produced and recorded; since defacers compete for attention and aim to alter frames in public debate, these aspects continue to shape their work and the recording of it.

Hacktivism as a form of critique of technology implies a utopian vision for such technology. It implies that technology can be used for something better, something more worthwhile can it currently is. To be able to make such a judgement about the better use of technology, participants need to have some kind of value system. It must be remembered from the discussion of open source just how much ideology is contained within the belief that unrestricted information will lead to better information. However, hacktivism is hardly defined by one single ideology but rather is a combination of different and at times contradicting strains and traditions. The most defining feature is an ideology of non-ideology, meaning that by naturalizing the infrastructure – in this case the ideal of a decentralized network – hacktivism presents itself as having overcome ideology. As the infrastructure is seen as the result of a natural, innate desire for free-flowing energy between equal participants, the network expression is seen as natural and ideology is understood as a restrictive measure of a restrictive, artificial society. This is most compellingly expressed in the Declaration Independence of Cyberspace:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. […] We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no

> moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. [...] Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. (Barlow 1996)

This key text of countercultural computing frames ideology as tyranny to be imposed by governments and in contrast presents the non-ideology of cyberspace as an advantage. There is no ideology, the text argues, mostly because ideology is an external influence which is unnecessary in a self-regulating network. This of course is a false consciousness masking the material conditions which underlie this brave new world. Habermas has already made this comment regarding bourgeois ideas of a non-ideological, free exchange (1989, 124), yet the conditions of cyberspace require further specification of this thought. It is not that technology is totally devoid of ideology, as Habermas explains:

> how is the depoliticization of the masses made plausible? Marcuse only had this to answer: Through technology and science also taking on the role of an ideology. (1976, 79 Author's own translation)

Critique of ideology in a network society, which is at the core of understanding hacking as utopian practice, is critique of the technology constituent of the network:

> In this sense, while resistance during the modern age forms around rigid hierarchies and bureaucratic power structures, resistance during the post-modern age forms around the protocological control forces existent in networks. Hacking means that resistance has changed. (Galloway 2006, 160)

The thought of hacking as a critique of ideology through engagement with the stratum (the servers and software) of the technology which is naturalized and has become ideology is key to understanding how and why any cybercrime archive exist. They are archives of past struggles and by providing a look behind the scenes of the brave new networked world constantly disrupt any attempts at naturalization.

Much of this literature review has been concerned with rooting hacking and hacktivism within their respective lineages. It argues against an exceptionalism of both the Internet as a medium and the practices and techniques associated with it. Being so embedded in contemporary technology and the managing of it, hacktivism is closely intertwined with existing structures of power and control. Defining it as antagonistic writing of electronic text describes hacktivism in its willing engagement with existing technologies for the creation of electronic text while driven by a vision influenced by techno-utopian romanticism about what texts should be written. This description of hacktivism situates web defacements as hacktivist practice. It illustrates the complex interactions between the practice of defacing websites, exercised power and the role of rational thought (as embodied in the critique of technology). During this process, a number of theoretical concepts have been borrowed from fields not traditionally associated with defaced web pages, and a number of under-researched areas have been identified. What this literature review adds to the thesis is a lens through which the research data may be observed. The upcoming methodological overview of the research process thus serves as a transition between the theoretical and practical parts of the thesis.

3. Methodology

3.1 Introduction

Web defacements as a form of hacktivism are rarely archived and thus mostly lost for systematic study. When they find their way into web archives, it is often more as a by-product of a larger web archiving effort than as the result of a targeted campaign. Aside from large collections such as the Internet Archive, which might pick up a few hacked pages during a crawl, there also exists a small scene of community-maintained cybercrime archives that archive hacked websites, some of which are hacked in a hacktivist context and may involve web defacements.

At the time of writing this dissertation, though, there exists no comprehensive academic archive of web defacements. The data sources that the methodology will extract material for the analysis from are distributed collections with varying temporalities (as most collections stopped adding new material) and collection foci (from all hacked pages to political defacements only).

As defaced websites are usually quickly restored, they can be seen as content especially vulnerable to deletion and as such depend on web archiving services to be preserved. There exists a range of different approaches to web archiving, most are specific to archiving goals and the nature of the material, be it static web pages, social media streams or short-lived image boards (Brügger 2005; Antracoli et al. 2014; Bragg and Kristine 2013). Specific approaches to ephemeral web material are described by Ball (2010), Healy (2017), McDonald (2015), and Ben-David (2020), with Ball describing a “performative model” for the presentation of complex web content, not exclusively ephemeral material:

> In this model, a researcher does not experience a digital record directly, but instead experiences a performance arising as a result of a process (software, hardware) running on some source data. In the Web context, a researcher looking at a Web page is in fact looking at a rendering of a collection of source files performed by a browser. (2010, 10)

In a study of content on 4chan, Ball describes ephemeral content as intrinsically competing for limited resources through excess:

> The ephemeral nature of posts [on 4chan] combined with their anonymity confronts the users of boards with a question of meaning – how does a board create a sense of shared experience, something that extends beyond the brief period that individual posts are present? Anonymity, combined with the ephemeral nature of posts, generates a dynamic of competition for the limited resource of attention: a driver of excess and the extreme. (2010, 12)

These characteristics of ephemeral content on image boards such as 4chan can be used to understand the nature of hacktivist web defacements; driven by a competition for the limited resources of visibility and attention, archiving defacements also serves as a tool to provide that shared experience. This explains why web archiving is important in this context and also hints at why community-maintained archiving exists within the scene.

In the following, I will further examine the difficulties of capturing, archiving and analysing ephemeral digital content, but particularly archived hacktivist projects. I will describe problems arising from the ephemerality and distribution of content. From this, I will identify the most appropriate model for conducting my study of defaced web pages as a tool of political communication.

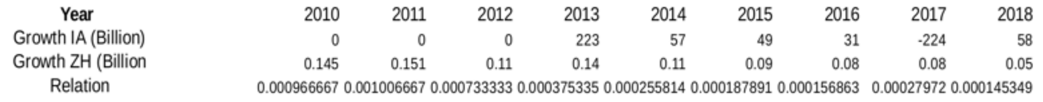
3.2 Ephemerality

In the context of existing, large-scale web archives, traces of hacktivism become part of the collection when the intended target site has been overwritten at the time of collection. Relating to the concept of antagonistic writing, one piece of electronic text was replaced with another, and that this new piece remained there while the site was archived. We cannot assume that whoever archived the page had any knowledge of this. In this context, finding traces of hacktivism that coincidentally were archived within larger grabs of web pages can be compared to searching for marginalia in books. Yet the analogy with a phenomenon borrowed from textual scholarship (cf. Jackson 2001) is only partially correct. If hacked websites are seen as part of a larger debate within a society, spanning from websites to social media to traditional media forms, it is true that this form of marginal writing can be “a truncated and imperfect witness to the remarkable popularity of [a] [...] topos or commonplace that circulated widely…” (Bawcutt 2015, 15). But looking at the individual site, the idea of marginal writing falls short of describing hacking and its communicative function, at least if understood as an addition. Understanding marginal not in the sense of writing on a margin, but in a postcolonial sense as writing from a margin towards the centre, hacktivism and postcolonial writing align in their attempt to collapse the empire by bringing the margin to the centre. Viewed in that light, hacktivists do not deface pages because they are unable to have their own online space, but because the act of disrupting a discourse of the centre is vital to their work.

While it is certainly true that hacktivism can be a form of engagement with a site’s original content in the form of a remix or parody, its style of engagement is also much more aggressive than that of leaving notes at page margins. We must also take into account that the majority of content on hacked sites is exclusive to the original content; one cannot be where the other one is. For these reasons, a better analogy to borrow from textual scholarship is the palimpsest, a pergamene page that has been scraped off and rewritten (Lyons 2011). Research on palimpsets includes forensic examination to restore the overwritten text and tries to establish a connection between the original and the new text. Similarly, forensic examination of digital media treats the existing data as palimpsets and aims to reveal the overwritten (Kirschenbaum 2012; Zielinski 2006).

Even if we are to take a step back and remove any notions of intent from web archiving efforts, we still have to account for the fact that hacked websites are, while certainly not uncommon, far outnumbered by uncompromised websites. Amongst this minority, a great part of which will be taken up by spam and malware, hacktivist activity is an even smaller subset.

To exemplify the magnitude of this, a brief look at the Internet Archive's Wayback Machine in comparison to a dedicated collection of hacked websites shows to what extent problems of scale affect the usage of large, general web archives for the research of hacktivist activity. Comparing the growth of the Internet Archive and Zone-H, one of the few remaining defacement archives, over the last 8 years shows that the ratio of hacktivist material one can realistically expect to find in larger, unspecialised web archiving projects is far below one percent:



Year	2010	2011	2012	2013	2014	2015	2016	2017	2018
Growth IA (Billion)	0	0	0	223	57	49	31	-224	58
Growth ZH (Billion	0.145	0.151	0.11	0.14	0.11	0.09	0.08	0.08	0.05
Relation	0.000966667	0.001006667	0.000733333	0.000375335	0.000255814	0.000187891	0.000156863	0.00027972	0.000145349

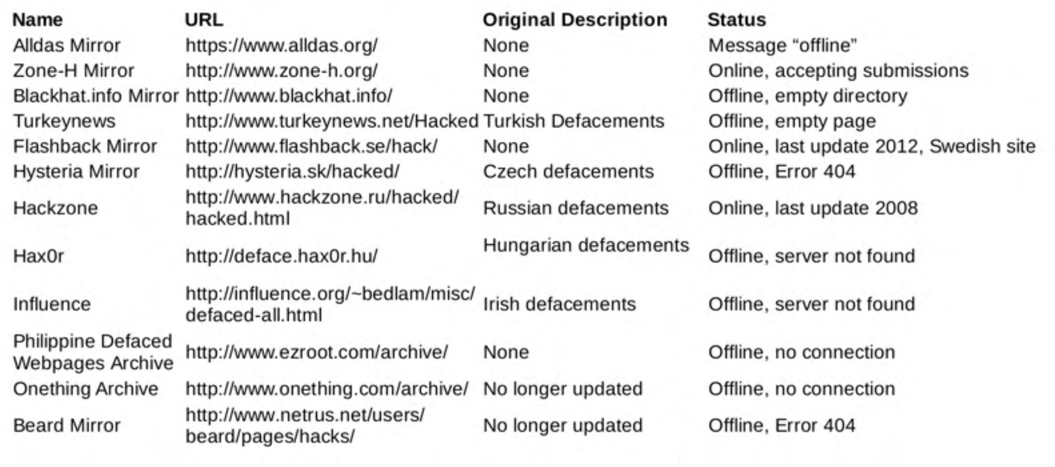
Table 3.1: Reported yearly growth rate of Internet Archive (IA) and Zone-H (ZH)

This is a somewhat crude comparison which does not take into account factors such as the availability of and changing efforts in web preservation, hacking or archiving of hacked sites. Nevertheless, it allows us to see the ephemeral nature of hacked content on the Internet. The ratios also remind us that archiving hacked web pages now is going to be harder than it was five years ago, due to the lower content ratio. This can be seen as a general point that can be made about the hacking of web pages, not hacking in general. Hacking might be alive and well, while the act of hacking a web page seems to have become more rare. Whether this means the process has become harder for some reason or motivation has declined is not clear from these numbers alone.

Hacktivism in the form of web defacements is not only hardly archived at the moment, but the existing archives are disappearing from the web. In her 2014 dissertation on hacktivism as a form of political participation, Samuel draws from archives that have since gone offline, while also dealing with a scarcity of sources herself:

> Thanks to the volume of defacements, the biggest mirrors (Attrition and alldas) have stopped archiving defacements. alldas has gone offline entirely; Attrition stopped maintaining its archive in April 2001 [...] but has preserved its records of defacements from 1995-2001. (2014, 8)

The mentioned mirror page, Attrition[16], has ceased to archive any new content but published a list of recommended mirror sites:



Name	URL	Original Description	Status
Alldas Mirror	https://www.alldas.org/	None	Message “offline”
Zone-H Mirror	http://www.zone-h.org/	None	Online, accepting submissions
Blackhat.info Mirror	http://www.blackhat.info/	None	Offline, empty directory
Turkeynews	http://www.turkeynews.net/Hacked	Turkish Defacements	Offline, empty page
Flashback Mirror	http://www.flashback.se/hack/	None	Online, last update 2012, Swedish site
Hysteria Mirror	http://hysteria.sk/hacked/	Czech defacements	Offline, Error 404
Hackzone	http://www.hackzone.ru/hacked/hacked.html	Russian defacements	Online, last update 2008
Hax0r	http://deface.hax0r.hu/	Hungarian defacements	Offline, server not found
Influence	http://influence.org/~bedlam/misc/defaced-all.html	Irish defacements	Offline, server not found
Philippine Defaced Webpages Archive	http://www.ezroot.com/archive/	None	Offline, no connection
Onething Archive	http://www.onething.com/archive/	No longer updated	Offline, no connection
Beard Mirror	http://www.netrus.net/users/beard/pages/hacks/	No longer updated	Offline, Error 404

Table 3.2: Mirror List based on https://attrition.org/mirror/

3.3 Availability and Preservation

Other problems of researching web defacements are availability and preservation of the pages. Availability here refers to any of the remaining site's long-term prospects. This includes funding, hosting and content review. Looking at Table 3.2, 9 out of 12 sites have already disappeared from the web. Many of them do not allow automated web crawlers to archive their domains, so that research cannot rely on larger, unspecialised collections to contain them. A further two archives are in a state of suspended activity and have not released any new content for 7 and 11 years respectively. It is reasonable to assume that these sites too will eventually disappear.[17]

The reason for this decline is unclear. A larger analysis of web defacements suggests web defacements have lost some of their appeal as a political tool (Balduzzi et al. 2018, 59). While this is likely to be one factor, a change towards web content being distributed through centralized platforms rather than individual web pages is certainly another.

My research cannot reverse this trend. It must simply acknowledge that the majority of content is irretrievably lost. What is left, however, must be professionally archived so that it can form the basis of further research. The methods used for this must reflect best web archiving practices and include as much metadata as can be scraped from the hosting sites. Some of the oldest defacements date back to the pre-2000s era and thus are a source which predates

[16] jericho, the admin of attrition.org, confirmed in an e-mail exchange that Zone-H holds a complete mirror of attrition.org’s collection.

[17] Defacements, in their complex relation between original page, defaced page and stabilizing community-based archive are of course also pieces of hypertextual writing and as such cross into the realm of early digital literature. On the topic, see Moulthrop and Grigar (2015).

the Internet Archive’s Wayback Machine collection. Only through proper methods of archival preservation does my own work have the potential to advance further research in the field. If the above loss ratio of sources is considered, it must be assumed to be only a matter of time before no more mirrors are active and all publicly accessible web defacement archives will become static web objects, and be eventually lost. This makes projects such as this timely interventions into digital heritage archiving.

3.4 Distributed Collections

Existing specialized archives in relation to hacking are independent collections of hacked and defaced websites. They are usually maintained by people with an interest in computer security, be it white hat (lawful) or black hat (unlawful) hackers or Internet activists themselves. Some of those archives are part of larger collection of sites based around computer security. Attrition.org, for instance, is:

> a computer security website dedicated to the collection, dissemination and distribution of information about the security industry for anyone interested in the subject. They maintain one of the only open and honest grim look at the industry, reminding everyone that we must strive to be better than we have been historically. The crusade to expose industry frauds and inform the public about incorrect information in computer security articles is a primary goal of the site. Previously, Attrition.org maintained the largest catalogs of security advisories, text files, and humorous image galleries. They are also known for maintaining the largest mirror of website defacements … (Attrition.org n.d.)

This critical view of “the industry” is often part of these site’s self-understanding as the outsiders who “get it” while the mainstream is ignorant or oblivious. This ties in with countercultural ideas of identity rooted in mainstream culture’s failure to anticipate developments. To labour Streeter one last time:

> When a marginal social movement accurately anticipates in the public eye a significant historical failure of judgment on the part of leadership, the effects can be powerful. Being right about something when the powers that by were wrong, for example, was a central collective experience of the 1960s counterculture; by 1969, the world had watched the television networks, the New York Times, and many members of the political establishment change their position on the Vietnam War. (Streeter 2011, 163)

This idea of being right where the established IT security is wrong, of seeing what the masses cannot or choose not to see, is important to many of these independent archives. Looking back on ten years of running the site, Zone-H also attributes to itself this knowledgeable underdog image:

> What also made [...] the site famous was its anonymous forum, especially the “0day rumors[18]” one, which became “the place” where security researchers and hackers came to brag or lie about their new discoveries. (Fernandez 2012)

[18] A 0-day describes a software vulnerability unknown to the vendor and public. Because of its novelty, it can be used for effective attacks on systems. Information on 0-days is sometimes traded at clandestine markets for considerable sums of money and used in intelligence agencies (Ferrell 2017; Zetter 2014).

The author then continues to explain how the site’s slogan was changed from “the Internet thermometer” to “unrestricted information” (ibid). This rebranding exemplifies the self-understanding of those archives not primarily as a deposit of information, but as a source of new developments. A thermometer is passive, reacting to external influences. The new slogan breaks with this image, suggesting that information freely flows from the archive, yet it also implies a restriction that looms over information in general and which may taint other, less determined and avant-garde, sources of information.

This framework may explain the immense dedication that went into building and maintaining these archives, not to mention the checking of every submission (Ferrell 2017; Zetter 2014). Checking every submission means adding another filter between input and archived content. The exact criteria for admitting to or removing material from the collection are crucial to know, yet no site has made them public. There is the option to see the submissions currently pending review, but no way to see material that was deemed unfitting for the archive. This filtering in general means that some kind of value system was employed which can range from technical requirements (the page was indeed hacked) to a more implicit bias towards certain messages, enforcing an echo chamber effect of approved submissions. There might also be practical considerations, such as not to allow content that would incriminate Zone-H such as attempts to incite or participate in an offence. For the most part, it has to be assumed that any content available has already gone through a filter.

To observe those archives and their content critically means to note some concurrent phenomena which appear in the majority of community-driven archiving efforts in the hacking scene. First, this is the role of the archive as a culturally affirming repository. The archive is not primarily the recipient of information, it is first and foremost the place where information comes together to form knowledge inaccessible to the institutionalized, slow understanding of the web. Those archives were created with the present in mind. They were places for people with similar interests to come together over material that was of interest at this very moment. What they knew or what they thought to know about cybersecurity was confirmed there, not created. There is no need to construct archives for users that already know the subject, hence the focus on a steady stream of content over archival curation. The slow and cumbersome analysis of the often poorly archived and described material is left to the scholars. Let them pick the crumbs out of the now empty echo chamber.

The second phenomenon which is telling about the nature and motivation behind these sites is their relation to freedom of information and freedom of speech in general. It is assumed that only through access to “unrestricted information” can one gain an “honest grim look” at the industry and – implied – act successfully in this environment. This mirrors open source ideology where access to the source code will benefit everybody and not just a small group of experts who can make sense of it. A critical perspective sees this multitude of unverified information not as constituent of public debate, but as eroding a common understanding of truth. It is very telling that the notion of truth does not feature in any “about us” section. This is because access itself is seen as a value through which truth, ignorant of the structures which determine public attention, will always rise to the top. This links back to Habermasian ideas of an inclusive, naturalized public sphere claiming to be governed by nothing but objective rationality.[19] In observation, web defacements are, more often than not the result of failure to participate in the envisioned public sphere. Habermas describes the consequences of failure to “mutually interpret” communication:

> if this attempt fails, one is basically confronted with the alternatives of switching to strategic action, breaking off communication altogether, or recommencing action oriented towards reaching understanding at a different level … (Habermas and Cooke 1998, 24)

This description fits the reality of web defacements since it describes communication as a relational and mutual act. As the following analysis will show, understanding communication as a relational and mutual act is often something defacers struggle with. The logical error of defacers to rely on a rationalized public sphere alone to recognize their arguments can easily be found by asking why, if access to information alone is constituent of public discourse, and publishing on the Internet is effectively free, there is any need to hack websites in the first place. This simple question then quickly reveals that neither access nor truth is the universal currency of defacements, but attention.

The third and last phenomenon is in sharp contrast to the second. It is the pseudo-Darwinist approach where the best hacker is the one bypassing the most advanced security systems, hacking the most pages, finding the most exploits. Hacker groups would, as shown by the messages they leave behind, be at war with other groups and try and hack their pages. In other words, those community-maintained archives see hacking as a competitive activity where an elite will dominate over the rest. This is the opposite of a goal of unrestricted information. Unrestricted access becomes access at the terms of whoever has the most capacity to influence the network. This situation would of course always be in flux, as to never allow total control of all pages, still the competitive overwriting of content is much more compatible with the echo chamber than the Habermasian public sphere promoted in the emphasis on information provision.

All those three phenomena contribute to the self-understanding of these community-maintained archived and their structure. The content they archive is determined by this self-ascribed gathering place of like-minded competitive hackers. It is caught in the conflict between being a live source and an archive at the same time, as much as it is determined by the conflict between being a place where truth can be spoken against censorship and being an arena where the most capable individual determines the rules. The content found in these community-

[19] For a Habermasian theory of rationality, see Habermas (1984).

maintained archives then is the realization of these principles. These aforementioned phenomena shape the structure and content of the archives, which, in turn, also delimits the scope of this study.

The status of these archives as community building tools means that, in terms of content, these archives all are volunteer projects, run by “cybersecurity enthusiasts”. This means all archives are labours of love, under-resourced and dependent on contributor’s free time and energy. Consequently, they may not be complete and are at the mercy of individual life circumstances of the archivists. Using them to look at the phenomena of hacktivism means the utilisation of an incomplete source, yet those archives also represent the most complete and raw view of hacktivism available.

The second trope of unrestricted information also has left its traces in the content and structure of the archives. Tying in with the first phenomenon, every archive is information that is hard if not impossible to verify as a whole and has seen very little curation effort. They are unrestricted in the sense that what they hold is mostly raw information – although there are, in fact, many restrictions which will be discussed in the next section. Again, this is in part due to the constraints these archives operate within but is also due to their self-understanding. The previously described notion of access as core value and prerequisite in the search for knowledge and truth means these archives choose to feature as much material as possible, even at the cost of accessibility. An alternative approach of having only a selected few pages archived and described in detail would have not been compatible with this emphasis on access.

Thirdly, structure and content are also influenced by the archive’s function as a leaderboard for competitive hacking. It is telling that the few bits of metadata available on Zone-H deal with the attacker more than the object (the website). Lists feature how many pages were defaced by what individual or group, with little attention being paid to the content that was overwritten. This leads to the object of my study – the web page – often being of only secondary importance for the designer and maintainer of the archive page. The defaced web pages serve as proof that something (the attack) was indeed carried out successfully, less so than the pages serving as a jumping-off point for a study of web security or the writing of antagonistic electronic text.

The qualities of ephemerality, availability, and complexity of both the archives and the content they house pose particular challenges for designing a research project to capture and analyse the substantive qualities of web defacement activity. Many best practices of web archiving (such as thematic scoping or of-the-shelf crawlers) could not be employed due to the nature of the target data source. As much as the technical side was very much characterized by a non-standard approach, research ethics also had to follow a custom approach as described in the next section.

3.5 Ethics

There are substantial ethical considerations when examining hacktivist materials. Research on and with hacktivist material is going to be research on the fringes of the Internet, as the content is only accidentally captured by means of web archiving, if not captured by dedicated archives. Thus, this study offers the opportunity to include little or unheard voices and perspectives into the historical record of the web. Ian Milligan describes the challenge and potential of using abandoned or ownerless web material:

> I feel similarly uncomfortable with leaving the voices of everyday people completely outside the historical record when there is ample opportunity to include them. Moving to a full opt-in process [referring to Geocities accounts] would likely lead to the historical record being dominated by corporations, celebrities and other powerful people, tech males, and those wanted their public face and history to be seen a particular way. (Miligan 2018)

Relating this to web defacements means to further expand the problem: hacktivist material is found within cybercrime archives, amongst a full range of gory images and defamatory content of all sorts. Not only can consent not be obtained, but the relevant material is hidden amongst plenty of other, largely unrelated websites. One explanation for this can be found returning to Ball, who understands “Anonymity, combined with the ephemeral nature of posts [as a] competition for the limited resource of attention: a driver of excess and the extreme” (2010, 12).

It is questionable whether this idea of competition can be directly applied to hacked websites, which by their nature appear to the viewer at random. Only when defacements are seen in a larger context is it that the competitive element of the attention economy appears. There is further complication in the phrase “excess and extreme” which does not adequately distinguish between signifier and signified. Pictures of atrocities and war crimes, often found in a context of accusation and calls for revenge, may be seen as representations of excess and extreme. It is in the context this material is used in which may be described as extreme, meaning outside of imagery or opinions usually featured in mainstream media. The label of extreme or excess in this case ultimately is a reaffirmation of values within a group. Those values will depend on time and place as much as the class regulating group communication. If hacking is understood as an attempt to subvert exactly this flow of communication, it is wrong to generally label it as extreme. Rather, to arrive at an understanding of why the object of my study is obscured by multitudes of tasteless and offensive content, we must look at the value of transgression in hacking and any countercultures in general.

Nagle (2017, 27–28) attributes transgression in online cultures to a cultural base which holds transgression and nonconformity as values in and of themselves. While this certainly is true for some forms of expression, with Nagle’s focus on the political landscape of the USA this approach does not describe how hacking may be used in cultures with a very different political system such as Pakistan or the People's Republic of China. Rather than explaining transgression through itself, and attributing its invention to the counterculture, it is worth going back further and understanding transgression as a potential to create alternate realities:

> Plato, followed by Machiavelli, believed that the security of political fabric woven by the lawmaker is best maintained by the seams of its construction remaining hidden […] the term [poetry] should be understood in its original Greek sense of poiesis, the productive use of words to conjure up worlds. In Plato’s day, playwrights were the poets of chief concern, but in our own day those adept at computer coding – ‘hackers’ – might be the main source of comparable subversion. (Fuller 2018, 33, 36–37)

Seeing transgression as this potential, it becomes clear why places such as these cybercrime archives, with a self-understanding of its user community as the secret avant-garde of digital utopians, would indulge in transgression. Combining this with hacktivism’s dual relationship with any perceived mainstream – disdain through the knowledgeable underdog image yet oriented towards it – produces an explanation of why transgression is so central and constituent to the object of the study.

With all that being said about the role of transgression, there is a fair share of content that would commonly not be seen as creating alternate realities, but rather as reinforcing negative aspects of the experienced reality of many. It is hard to quantify aspects of discriminatory content in hacktivist site defacements. Whether reports of gender discrimination and harassment experienced by hacking conventions (Richterich 2018) can be seen as the underlying theme of the scene and translated onto hacktivism is uncertain.

What is certain, however, is that reliance on one single archive, such as in the case of this study, carries the risk of reinforcing limitations and biases already present in the source material. In other words, we must not forget Zone-H's original function as a community site and leader-board for competitive hacking. This means that material found within the Zone-H archive is likely created by individuals who felt drawn to this competitive scenario and who saw value in engaging with their fellow community members in this way. Further, whenever discussing the heterogeneity or diversity of defacements, it must be considered that a certain amount of privilege was necessary to be active on the Web of the early 2000s. This privilege may take the form of available time, equipment, Internet access and English language skills and is oriented along the general lines of privilege and opportunity within a society.

Another limiting factor is the exclusive focus on English language defacements, omitting a large share of Spanish and Portuguese language, and a smaller share of German language defacements. Especially when discussing political orientation towards Western liberal values amongst hackers, this selection bias must be kept in mind. Future expansions of this research project should therefore aim to diversify the range of sources to overcome such selection biases.

Using NLP to analyse defacements brings with it the risk of entering a confirmation bias circle, where the tools geared towards standard English language expression overemphasize defacements featuring such standard English language expression. The more the analysis is externalized in this way to automated tools – for example, sentiment analysis or named entity recognition – the greater this risk becomes. It is important for research to acknowledge this risk and critically assess any automated content analysis.

It must further be considered that some forms of hacktivism are illegal. The definition of cybercrime varies between jurisdictions, so for the context of this thesis all unauthorized alterations of any website will be considered illegal. While my research is focussed on the communicative function of defaced websites and not the technical conditions of the hack, it must be considered that the object is not only a collection of occasionally tasteless websites, but that in some cases considerable damage was done to the target system.

Beyond the potential for legal persecution, the research object is further complicated by questions of consent. It can generally be assumed, when working with material either obtained through a general or specialized archive, that hacking of any web page is done without the owner's consent. This is hardly an epiphany but should be kept in mind when deciding how to engage with hacktivist content in a scholarly context. While this is not human subject research, but research into texts that by their nature were intended to be public, there are still considerations of consent to take into account.

When dealing with defacements, we have to consider that there are at least three distinct layers involved. Each layer represents different types of authorship, different expectations of privacy and publicity and different levels of agency and vulnerability. What all three layers have in common, however, is that none left a signed form expressing their informed consent. These layers will be explored in more detail below and show how ethical considerations when dealing with defaced websites shape the research methodology.

The first layer is the original website. In some cases, an attacker would create a parody of the original page, featuring the original layout and re-using some of the content. In all cases, the target URL would give indication as to who the original owner was. In some cases, this could lead to identifiable information about the original owner, for example when the target URL is something like michaelkurzmeier.com. These original owners of the digital frontier did not consent to having their page hacked and/or having their content re-used in any way. I had to thus design the focus of my study in such a way as to not use any identifiable information in URLs by focussing on top-level-domains instead, and to not include any parodies of personal websites. These original owners are the most vulnerable group and special consideration must be given to protect them.

The second layer is the attacker. Even though I considered it safe to assume that hackers deface websites with the intention of creating some publicity, I had to consider the fact that attribution of attacks is not always straightforward and that attribution could cause harm to individuals. For the study design, I had to mitigate that risk by only providing as much information as defacers were willing to share through their work or their dedicated homepage. This group has of course very different expectations of privacy and publicity, yet their needs must also be considered.

Finally, the last layer is the content layer. For this, it is important to understand that – as Samuel (2014, 105) states – defacers go shopping for an ideology after they decide to become defacers. This, and the fact that defacements are often done en mass, means that content from and about all sources can be found even in political defacements. From pictures to identifiable information about 3rd parties to copy and pasted texts. This means that all content had to be screened for identifiable information. While most pictures turned out to be already public press photographs, I still decided to not include any identifiable information of any kind.

This three-layered approach breaks down intersecting ideas of authorship, consent and responsibility in web defacements. It can also be used to more generally understand web sites as the intersection of different authors' contributions, all with their own and possibly with very different expectations for privacy and specific needs. The ethics of deletion, that is the question of what to deliberately include and exclude in a web archive, can benefit from this discussion of layered content in web pages since it acknowledges that most websites are collaborative works and the discussion thus highlights the need to identify and find appropriate solutions to each layer.

Therefore, even though an approach may be metadata-based and without personal identifiable data, the potential risk to involved parties must be understood and must be considered. While metadata seems like a convenient concept to avoid ethical conflicts, the distinction between original and meta data is not as clear-cut as it may seem. For Zone-H, the target URL and IP are part of the metadata and could easily provide personal and identifiable information. Further, some parts of the metadata may be falsified either by the attacker or the target for a number of reasons as will be discussed in more detail in the following sections.

The first question derived from this is the medium itself. Maynooth University Ethics Policy states that

> The consequences of research may reverberate at many levels, including the local community of participants, the professional community and the wider society. Researchers should be cognizant of this and sensitive to issues arising from inequalities of power. (Maynooth University Research Ethics Policy and Committee 2016, 12)

This responsibility explicitly extends to the professional and private community of owners of hacked websites. It should be considered, especially in the case of smaller websites, whether the URL needs to be provided to understand the hack or whether the owner could be exposed through it. In many cases, it will be sufficient to briefly describe the site to provide context.

It is also a key question in web research whether information is to be treated as text as personal expression. Stine Lomborg acknowledges that:

> [for] the study of the development of specific sub-cultures on the web (e.g. sexual minority groups, political extremist debate fora or camgirls’ websites), using archival data on the participants and their online communications may be more problematic, if only because of the risk of exposing and causing harm to specific private individuals, based on their prior affiliation to a sub-culture. The case-by-case ethical judgement starts with reflections about the textuality or humanness of the data in question. (Lomborg 2018, 102)

According to Lomborgs’ argumentation here, the use of hacked sites could potentially be problematic insofar as legitimate site owners might be – against their will – affiliated with cybercrime. This can be mitigated by shifting the focus more towards the hacktivist material and less to the original page.

The second aspect is the posted material. It is entirely possible to come across personal information that was posted for no other reason than to expose and humiliate a person. Although such sites will hardly be hacktivist content by definition, it is also a requirement of the research design to exclude any identifiable information as consent cannot be sought or assumed. In the same way, other identifiable information such as photographs must be dealt with using great care and consideration. It is in the absence of ethical guidelines for engagement with hacktivism that those principles had to be derived from general ethics guidelines.

A departure point for the development of general ethical standards in engaging with hacktivist content is the Association of Internet Researchers (AoIR) ethical guidelines. The document is considered a guideline for the diverse and evolving field of Internet research. It acknowledges the difficulty of obtaining informed consent in a large-scale data collection:

> consent is manifestly impracticable in the case of Big Data projects, however, resulting in a serious ethical dilemma. […] Some researchers are trying to obtain first-degree informed consent, others are focusing on deleting names and other highly identifiable information from the dataset when storing and processing the data. (Bechmann et al. 2020, 10)

The authors suggest a method called data minimization (Bechmann et al. 2020, 20) to reduce the risk of releasing sensitive or identifiable information. With this method, only non-identifiable content relevant to the research question remains in the data set. As the research data for this project potentially engages with sensitive data obtained without the original owner’s permission, the principle of data minimization provides a way to minimize risk.

Note that the AoIR guidelines naturally are general guidelines and may not necessarily meet all the requirements for a specific research situation. In the context of this thesis, the question of how to ethically engage with hacked websites and their content must be answered. Poor and Davidson draw parallels to Edward Snowden’s release of NSA documents:

> In one prominent example, journalists published classified American security documents that Edward Snowden had released without authorization. Members of the Association of Computing Machinery (ACM) debated the ethics of Snowden's actions, and those of journalist Glenn Greenwald. As they pointed out, Snowden's actions were clearly illegal and a breach of both workplace ethics and rules. Some pointed out how any whistleblower will be violating at least some ethical rules and perhaps laws as well, in the hope of stopping a greater wrongdoing. (2016, 3)

The connection is then made to their own work on the crowdfunding website Patreon and the ethical concerns about using user data obtained through a hack of the site's database. The authors then explain their decision not to use the data leaked through the hack as they assume that the now public data was initially meant to be private (Poor and Davidson 2016, 5).

As much as I share Poor and Davidson's position about the original data owner's intent, it is necessary to explain important differences between using data obtained through hacking and data about hacking in my research. All content available on Zone-H was a public website at one point. I relate this situation to the concept of "expected privacy" as defined by Milligan: "Did the author of the individual website they [researchers] are citing or using as evidence have a reasonable expectation of privacy?" (2018). Defacers hack websites with the intention of creating as much publicity as possible, even more so when they submit their work to be archived. While it is possible to come across identifiable information, this is not the focus of the study and this information will not become part of the dataset under the data minimization principle. With this approach I am able to bridge between the impossibility of obtaining consent and the data collection principles outlined by the AoIR.

It is also, and importantly, not possible to confirm a defacer's identity. This means that apart from hints such as style, topic, date and target, there is no definitive proof that any of the defacers are who they pretend to be. Anybody can submit defacements under any name and it will be up to the archive if those false attributions are ever resolved if at all. This complicates the research as names become less reliable and identification has to rely more on content and context than on clear attribution. Samuel (2014) conducted interviews with web defacers, Coleman's work on Anonymous (2013) also features extensive interviews with some participants. Finally, Hopkins (2014) completed a *Virtual Graffiti* project based on content from Zone-H. All these works relied on voluntary contributions from within the scene and of course did not in any way attempt to officially identify participants. Following those works, the research on Zone-H defacements will take attribution seriously whenever possible but will also understand that assuming or hiding one's identity is part of a continuous process of transgression and will use hacktivist public names as given throughout.

3.6 What is a website?

A key unit of analysis in this study is the website, but it is surprisingly difficult to arrive at a working definition of what a website is. This is because there is no one website object, but multiple objects interpreted by humans and machines. Settling on one definition is perhaps the most complexity-reducing step, as it determines eligible data and methods.

A website on a technical level is one or more files. This includes simple, static HTML pages as well as refined, backend-dependent interactive sites. It is typical for an HTML document to reference other documents, such as CSS files, images, or other HTML documents. Some of those are links, some form vital parts of the site. These referenced files may contain information which is not present in the HTML, thus focussing on HTML alone is a type of limitation of complexity by itself. Drawing a distinction between HTML, images and links is significant since limiting the capture to only HTML allows the storage of many thousand pages on any current hardware and also opens up the possibility of processing the captured data through textual analysis.

A general problem with an approach focussed on files found at a given address is that content will always be excluded if it is embedded from a 3rd party source. Embedded video, for example, will not be captured. The same is true for scripts loaded from 3rd party sites, even though security considerations should exclude script execution from the start. Finally, this approach reduces all websites to their pure textuality and ignores all visual elements. It is not that HTML is incapable of displaying visual information, but rather that to a textual analysis tool any image will be little more than its file name and description.

On a phenomenological level, though, a website is not pure HTML but what appears in a browser. To analyse a website through this approach is somewhat more complicated since the actual user experience may depend on a number of factors, including

- operating system and browser
- setting and installed fonts
- device (many websites look differently on phones and tablets).

There is no clear distinction between files and referenced content. A user may experience the seamless integration of video content, even though the video is part of another site. On the other hand, a user may not experience certain things, most prominently ads, if they have changed their configuration accordingly. The user experience is also only a fraction of the content that is contained in the HTML files. HTML tags obviously exist so that they are not shown in writing but interpreted by the browser and visualized for the user. Comments are human-readable writing within the files that serves no technical purpose but may still convey meaning. Images feature a description that is only made visible when the image itself cannot be loaded.

General problems with an approach focussed on the phenomenological can be divided into a technical and an analytical side. Technically, a phenomenological approach allows for very little automation as the object only appears through observation. As experience is emphasized over textuality, visiting each website becomes a necessity. This can partially be mitigated through the use of automated pattern recognition software, but even such software is merely an attempt to bring textual analysis in disguise back into phenomenology.

Further, this approach also suffers from the fact that certain elements might not have been archived and thus are missing. An interface is only ever a dip into a deep well of data files in the underlying database infrastructure from which each interface is generated. Out-of-scope would be embedded videos, 3rd party scripts and externally hosted images. Capturing all these elements would require significantly more space and would in turn greatly reduce the number of sites analysed.

Both approaches must be combined in the right order to combine their strengths. The first is the decision to limit the depth of links to follow, and of how to deal with embedded material. Secondly, it is the sequence of filtering data. In my model, textual analysis through software is the first step in surveying a large number of websites. Once hacktivist defacements have been identified, a second step is to look at them in term of their discursive function.

Textual analysis can also be effectively used to filter out large quantities of unwanted data. Combined with the provided metadata, textual analysis can provide word frequency over time, to visualize web responses to political developments. Automated grouping of words can help overcome the lack of standardization and uncover relations between phrases and hashtags.

As much as a website is a combination of technological, material and phenomenological layers, traces of hacktivism can be found on all of these layers. Ephemerality and the antagonistic nature of web defacements also makes them harder to find than other types of web content. The next section will thus be focussed on how metadata description can help find and categorize defacements.

3.7 Metadata

The next challenge in examining defaced web pages is how to describe the data. Description through metadata means more than the simple availability of metadata. It means the availability of a standardized set of tags associated with the archived object. Both metadata and object must be combined to provide independence from the archival infrastructure. In web archiving, this is best achieved through Web ARChive (WARC) and Web Experience Toolkit (WET) files that store metadata in the same place together and with the archived object.

Previous sections have begun to sketch out the process of selection and scoping of data, yet what is missing still is a robust system for describing data. In relation to the web defacement mirrors listed in Table 3.2, it might be argued that some of the material already is available online. This is only partially true. First, as the status overview shows in Table 3.2, most pages are no longer live. This means that with each passing day the percentage of captured material diminishes. Even if the records for a certain phase, say the early 2000s, were assumed to be completely available, their preservation and integrity are dubious. This means that we have no way to verify any of the collections against a target list, we are not able to see the results of the crawl and we cannot make any statement as to how many pages failed to archive and for what reason. This further emphasises the point that the archive is incomplete, yet the extent of the gaps is only to be estimated.

This is all in relation to the second point, the lack of metadata. Metadata is partially missing for the individual pages. Description through metadata means to create and use metadata in such a way as to describe the content of a page to make it accessible for human and machine analysis. In the case of Zone-H, for instance, there are some parts that would qualify as metadata, yet it seems great care has been taken to separate these from the actual content. This metadata is not searchable; only notifier name is. Further, all data available strictly refers to the notifier (such as time, date, operating system etc.) but none refers to the page itself, indicating such things as motivation, type of hack, referenced organisations. It might be that this is the lamenting of a researcher looking at a collection brought together by very motivated individuals in their spare time, and it might seem overly demanding to ask for all this metadata to be captured for each page. A lamentation it might be if that exact information were not asked for with every submission and then presented in annual statistics. The problem of keeping the metadata away from the preserved object strikes yet again, making it impossible to connect parts of the agglomerated metadata to the objects they were derived from.

To be searchable and to allow for agglomeration of data, the metadata description of any object must follow a universal standard. This metadata description can be seen as an additional layer of abstraction which allows for uniformity where originally there was none. Through the layer of metadata, the objects become uniform enough to be agglomerated and automatically process yet retain enough of their difference to be combined to conclusions.

The usage of metadata determines the future use of the archived objects. Missing out on important items would mean to seriously limit the future use of the archive. Similarly, setting the groundwork with a good set of metadata definitions will enable interoperability. In the following sections, a metadata schema for the description of hacked websites will be described. What will be described is a model of analysing websites that are ephemeral, partial, badly preserved, have complex ethical considerations and limited existing metadata that involves a custom metadata creation process. This model will be the basis of the applied methods described in the following section.

3.8 Justification of chosen archive

Given the difficulties in identifying a singular source and that hacker activity exists primarily in the form of ephemeral traces, it was necessary to survey a range of archives that hold web defacements and find mechanisms to filter web defacements for the sake of this project. A range of sites were surveyed, based on Table 3.2:

Name	URL	Status
Attrition	https:// www.attrition.org/	Stopped accepting submissions, archive open to research. Collection mirrored by Zone-H.
Zone-H Mirror	http://www.zone-h.org/	Online, accepting submissions
Flashback Mirror	http:// www.flashback.se/hack/	Online, last update 2012, Swedish site
Hackzone	http:// www.hackzone.ru/ hacked/hacked.html	Online, last update 2008

Table 3.3: Surveyed online cybercrime archives

Of these sites, it was decided to focus this study on Zone-H for the following reasons:

a) Maintenance status: Zone-H still accepts new submissions, meaning there seems to be some effort still being put into the site which was understood to lower the risk of the source disappearing mid-crawl.

b) Collection size: Because of the ongoing new submissions, Zone-H offers by far the largest collection of defaced webpages. The collection is extensive both in the time period covered, as well as regions/languages and depth.

c) Stewardship of other collections: Zone-H features material that originated in other, older archives such as Attrition.org.

3.9 Justification of focus

The scope of the data collection had defined to be in a range where a substantial amount of data was captured to ensure representative conclusions to be drawn from the data, yet in a range that would allow processing within the time frame of the thesis. As part of this thesis' approach is the experimental application of automated data processing, the available amount of data had to be in a range where manual survey was achievable to confirm findings from Natural Language Processing. As the following sections will explain in detail, scraping the archive was a slow process of approximately 800 pages per day, so that for the practical purpose of completing the thesis in time the focus had to be adjusted.

The collections process was designed to start at the lowest DefacementId Zone-H has assigned (DefacementId 1) and move upwards in batches of 1000 defacements. This would produce a complete capture of defacements from approximately 1999 to 2001. To further ensure that this data set was representative of the entire collection, a further 2 batches of 1000 defacements each was randomly selected from the remaining time periods in the archive and captured. While this qualifies the findings of this study a little – as it cannot be guaranteed that the studies corpus is representative – it helps to ensure some semblance of representativeness while retaining achievability.

3.10 A hacked-together approach

3.10.1 Workflow

The following section will guide the reader through the process of creating the dataset keeping in mind the considerations outlined above. It begins with the process of crawling the available material and follows the outlined workflow to explain the steps undertaken.

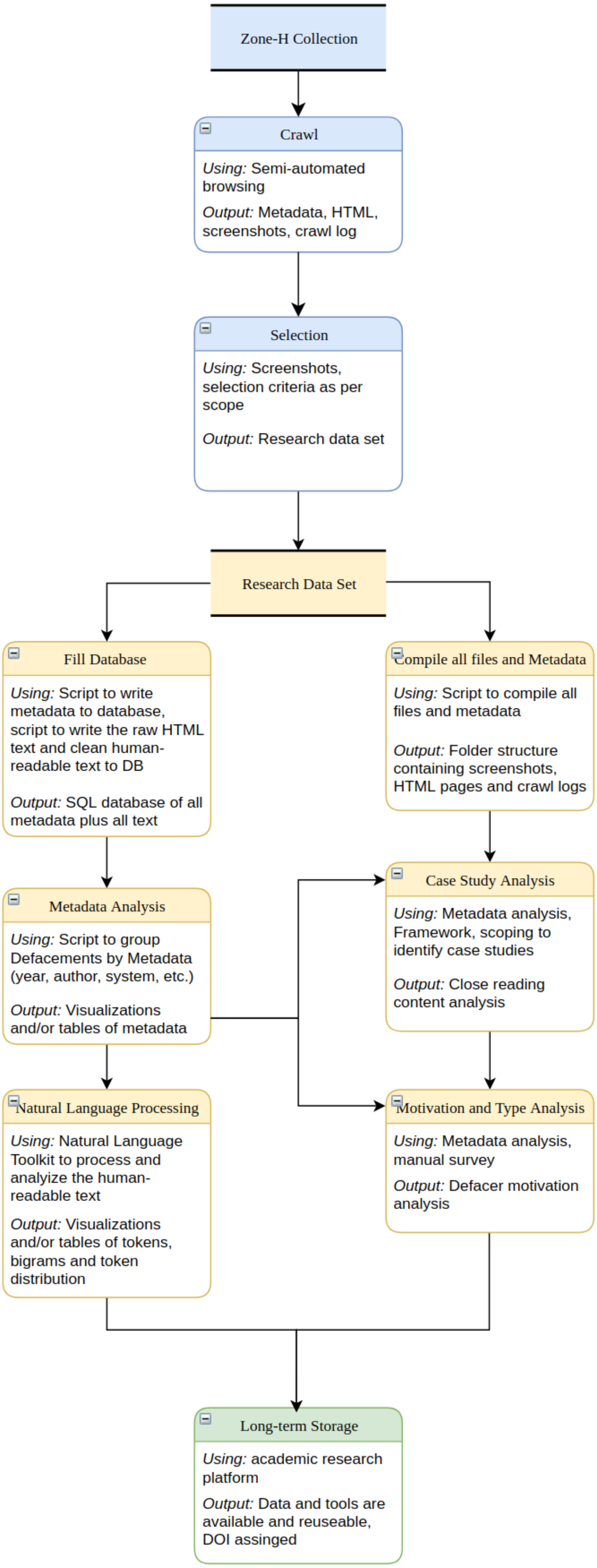

Zone-H Collection
Crawl
Using: Semi-automated browsing
Output: Metadata, HTML, screenshots, crawl log
Selection
Using: Screenshots, selection criteria as per scope
Output: Research data set
Research Data Set
Fill Database
Using: Script to write metadata to database, script to write the raw HTML text and clean human-readable text to DB
Output: SQL database of all metadata plus all text
Compile all files and Metadata
Using: Script to compile all files and metadata
Output: Folder structure containing screenshots, HTML pages and crawl logs
Metadata Analysis
Using: Script to group Defacements by Metadata (year, author, system, etc.)
Output: Visualizations and/or tables of metadata
Case Study Analysis
Using: Metadata analysis, Framework, scoping to identify case studies
Output: Close reading content analysis
Natural Language Processing
Using: Natural Language Toolkit to process and analyze the human-readable text
Output: Visualizations and/or tables of tokens, bigrams and token distribution
Motivation and Type Analysis
Using: Metadata analysis, manual survey
Output: Defacer motivation analysis
Long-term Storage
Using: academic research platform
Output: Data and tools are available and reuseable, DOI assinged

Figure 3.1: Workflow

3.10.2 Crawl

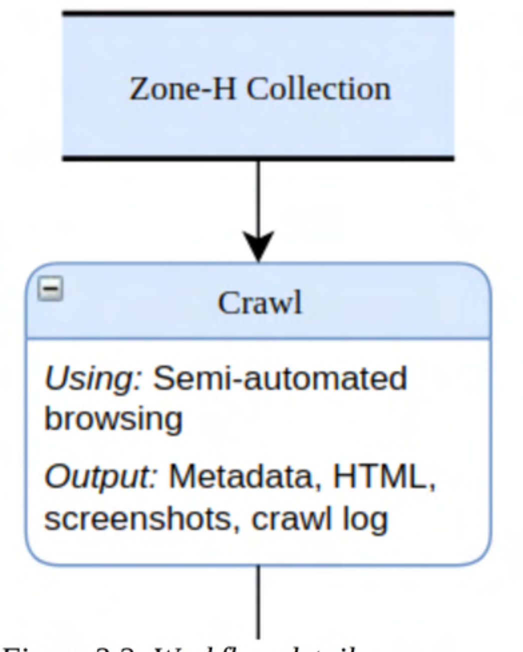

Zone-H Collection
Crawl
Using: Semi-automated browsing
Output: Metadata, HTML, screenshots, crawl log

Figure 3.2: Workflow detail

A semi-automated web crawler was developed by me[20] to browse through the archive and collect the HTML source of the defaced page together with the provided metadata. A screenshot of the defaced page was taken to allow for quicker visual orientation and also with a view towards publication of the research data. A log file was kept for the entire crawl process. Data was stored in batches of 1000 pages, together with the log files and the metadata. The crawler in its first iteration was a command-line tool which provides the greatest level of flexibility and access for further development. To ease access to the research methodology, a graphical interface was later developed.

During the design process for the crawler, a question very specific to the content of these cybercrime archives had to be dealt with. The question was whether it was better to design the crawler to stay as true to the source as possible, meaning enabling all scripts and capturing the page with all its contents or to disallow all external requests and focus on the bare HTML. This question ties in with the earlier discussions about the constituents of a website and was suspected to be especially important for defaced pages since it was assumed that defacers would make frequent use of externally-hosted material. This factor is called depth in web archiving. Common settings would be to follow all links on a target domain recursively and to follow links on other domains up to a depth of 1. In an example case, a crawler might start at www.maynoothuniversity.ie and capture every link that is on that domain such as www.maynoothuniversity.ie/library and www.maynoothuniversity.ie/research. It would then continue searching for links that are on the maynoothuniversity.ie domain until eventually it would run out of new links to discover. If any external sites are linked, such as www.ucc.ie, the crawler will only archive the exact linked page and will not go looking for more links on the ucc.ie domain.

The decision of how to set the depth parameter is usually influenced by the expected content and aim of the crawl. If the goal is to accurately archive a whole domain with all embedded content, even at the cost of increased size, the crawler might be set to fetch all on-site links recursively and all off-site links to a depth of 1. If only a single page is to be captured, the crawler might be set to crawl on-site

[20] A detailed description of any programs, databases and scripts used is found in the following section. The repository containing all self-developed crawlers and scripts is available here.

links to a depth of 1 and ignore all off-site links. Many combinations of the two settings are possible, but the underlying logic is that more depth will produce more output.

Off-Site Links	recursive	>1	1	0
On-Site Links				
recursive	Possibly infinite number of links, not possible	Very high number of links grabbed, extremely large collection, not practical	All on-site links grabbed, default setting for most web crawlers	All on-site links grabbed, no external content. Useful to limit collection size and control content
>1	Possibly infinite number of links, not possible	High number of links grabbed, focus shifts from on-site to off-site	High number of on-site links grabbed, useful for large sites such as forums	High number of on-site links grabbed, no external content. Useful to limit collection size and control content
1	Possibly infinite number of links, not possible	High number of links grabbed, focus shifts from on-site to off-site	Only one page crawled plus all referenced material, useful for focussed archiving	Only one page crawled, useful for focussed archiving
0	No links grabbed	No links grabbed	No links grabbed	No links grabbed

Table 3.4: Crawling depth comparison

In the case of Zone-H, it is just one page I was interested in. On-site links could thus be crawled with a depth of 1. Off-site links, however, presented a quite specific problem. As described, off-site links are resources referenced on the original page. This might be a video that is central to the defacer’s message or a script for altering the page’s layout. Some of the many thousand pages in the archive also feature malicious code such as endless pop-ups (annoying but harmless) or viruses (potentially dangerous)[21]. So, the general design question was whether to not allow off-site links and risk missing out on some content for the benefit of a more stable and safe operation or to stay closer to the source and require a constant manual control of the crawl. For the sake of being able to run the crawler more smoothly, it was decided to take a restrictive approach. Zone-H also does not archive any off-site content (for reasons not stated) so that mixing the archived on-site content with live off-site content would have resulted only in further complications without necessarily adding new data. The selected settings were: On-site 1, off-site 0.[22]

The dataset was created using a two-step process. First, as described above, a large number of defaced pages were saved. Usually, saving web pages means to send automated requests to a server and to store the reply. This method relies on a command line interface, meaning that no scripts are executed and no graphical information is exchanged. In the case of Zone-H, this method was not possible. Zone-H's archive relies on the visitor's browser to construct the page as it is being accessed. This means that for every page, there is a short waiting period during which the screen is empty. Further, this means that a command line interface tool would not construct the page and only capture the empty loading screen. Because of this, data could not be collected using common web scraping tools such as HTTrack[23] or Wget[24], but automated browsing had to be used as a method.

Automated browsing means to have a program control a browser to access web pages, select links and save elements. This method allows the page to be constructed, it gives the user the ability to specify a waiting time and it is more likely to look like a legitimate visitor to a site's security systems. As a downside, this approach is much slower than a text-based tool and more complex to develop. The program I developed uses the Selenium Webdriver[25], a Python framework

[21] Writing from an IT security perspective, Balduzzi et al. describe how defaced websites can be sources of malware – either in a conscious attempt to spread it or because defacers themselves use compromised machines (2018, 56–57).

[22] As I see the archiving of these pages as critical for their future use in any academic environment, a second crawl of Zone-H has been started. This crawl uses an established web archiving process to revisit all URLs from the first crawl and capture the full page file together with crawl (but not defacement) metadata. This is equal to a crawl with the settings on-site 1, off-site 1. This has the potential to be more complete as all referenced material will be included, given it is still available. This referenced material is the reason this crawl is a special case. While with all web archiving efforts, elements of cybercrime such as malware may be anticipated, this one is focussed on such content. Some special preparations were undertaken to ensure successful operation. The benefit of switching over to an established web crawler is that it is robust enough to handle web design elements such as endless pop-ups. Since in this second visit referenced material is being included into the web archive files, the crawl will have to be run inside a virtual machine and all captured pages are to be seen as potentially containing malware. This is because amongst the referenced material loaded from off-site links will certainly be a percentage of malicious content. This does not mean that the material becomes unusable, but that it needs to be treated with the adequate safety measures in place.

[23] **HTTrack** is a versatile web archiving tool, see https://www.httrack.com

[24] **GNU Wget** is a command-line tool to download files via HTTP, HTTPS, FTP and FTPS. Many web archiving tools are built using Wget. See https://www.gnu.org/software/wget/

[25] **Selenium Webdriver** is an automated browsing solution, whereby a web browser such as Firefox is controlled by a program. The main difference in the context of this thesis is that

initially made for automated testing of websites. The program has the following logic:

```
First, the user selects how many pages the program should
attempt.
For every page:
      Try to open the URL:
            If successful:
                  - Identify metadata (Date
                  submitted, attacker, system, etc)
                  and write it to the output list.
                  - Access the defaced page and
                  take a screenshot.
                  -Save the page as a text file.
            If unsuccessful at any step:
                  - Write the URL and reason for failure to the
                  error list.
```

At any stage, the program has to be able to handle pop-ups and dialogue boxes which some hackers felt were indispensable elements of web design. It also must be configured to run scripts from Zone-H (so the page can be constructed) but from no other source. This is done by loading NoScript[26] into the browser to prevent the execution of scripts from 3rd parties. The program is robust in that it can be interrupted at any time without data loss. It was said earlier that Selenium Webdriver is a framework for automated browsing. This is true, but Zone-H still has ways to limit the usage of automated solutions:

The first limit is the soft limit of requests per day where the site would require users to complete CAPTCHAS approximately every 80 pages. This means there needs to be some supervision of the browsing process. These CAPTCHAS cannot be solved by Selenium Webdriver.

The second limit is a hard limit of requests per IP where after about 800 URL visits, the IP would be banned for 24 hours. This meant that crawls had to be spread out over time. There is a disclaimer to contact the administrators if users received an unjustified automated ban, however there was no response to my requests to exclude my IP from that request limit.

A distinguishing feature of Zone-H is the age of its collection. In web archiving terms, Zone-H holds some of the oldest known defacements. These defacements date back to 1999 and were carried over from an earlier site, alldas.de. There was mention of Zone-H working on incorporating material from attrition.org dating back to 1995 however this material has not been incorporated into the site yet (Fernandez 2012).

To adequately cover these early defacements, the crawl would start at DefacementId 1 and increment that number to move from the oldest towards the

automated browsing can capture elements which are only constructed on the client side – it is a “what you see is what you get” solution.
See https://www.selenium.dev/documentation/en/webdriver/

[26] **NoScript** is a Firefox extension which can prevent the execution of some or all scripts on a website. See https://noscript.net/

most recent material. While the DefacementId is not an exact indicator of a defacement's age – rather it shows the sequence in which material has entered the archive – it correlates with time and date reasonably well enough to be used as an indicator.

Occasionally, a DefacementId would lead to an error or empty page. This rarely happened in the first 10,000 Ids, but grew into a problem eventually. Every invalid DefacementId would count towards to the URL request limit mentioned earlier and also slow down the crawl considerably as the script would wait for the page to load. As these invalid DefacementIds tended to occur in larger groups, the following logic was implemented into the crawler:

```
If a capture fails due to an invalid DefacementId:
      Skip forward a random amount of DefacementIds between 1
      and 10.
      If the next capture fails again due to an invalid
      DefacementID:
            Skip forward a random amount of DefacementIds between
            10 and 100.
            Repeat until a valid page is captured.
```

Metadata available on Zone-H reflects on the site's communicative function as an echo chamber rather than an archive. What is available is listed in the following table:

Metadata	**Description**
Date	The time and date the URL was saved by the crawler
Notifier	The person submitting the URL
Domain	The original URL
IP Address	The IP address of the notifier. This is apparently used to confirm the identity of the notifier and to automatically assign a country
System	The operating system of the defaced page
Server	The web server application of the defaced page
Country	Derived from the IP, if available, displays a nation's flag based on IP location

Table 3.5: Metadata captured from Zone-H during the crawl

Pages originating on alldas.de do not feature values for IP address and country. Supposedly that is because alldas.de did not record these values. Material originating from the alldas.de archive is also marked with the HTML commentary

```
<!-- Mirror of this Defacement provided by
http://defaced.alldas.de – >
```

As part of the scraping and in preparation for the analysis, I have added the following metadata attributes:

Metadata	**Description**
MirrorURL	The URL of the archived page
DefacementId	Derived from the URL, a unique identifier for each defaced page
InScope	Binary value to describe if a page meets the criteria to be in scope. This will be filled in the following step.

Table 3.6: Added metadata attributes

The output of the crawl process is thus:

- The HTML files and screenshots obtained
- The log file describing the crawl process
- The list of metadata captured for each page

With this data, the next step was the selection of material for the research dataset.

3.10.3 Selection

The vast majority of pages scraped in the aforementioned process did not meet the definitions of pages defaced in any hacktivist context. That is due to the fact that the targeted archives are general cybercrime archives rather than specific hacktivism archives. Thus it was necessary to manually select which pages fit the description. The crawler design supports this task by providing a screenshot of each page, which means an initial visual survey of pages could be carried out quickly. Results from this initial selection process were combined with the rest of the scraped data for further analysis. The selection process must also consider the ethical limitations of the study as described earlier.

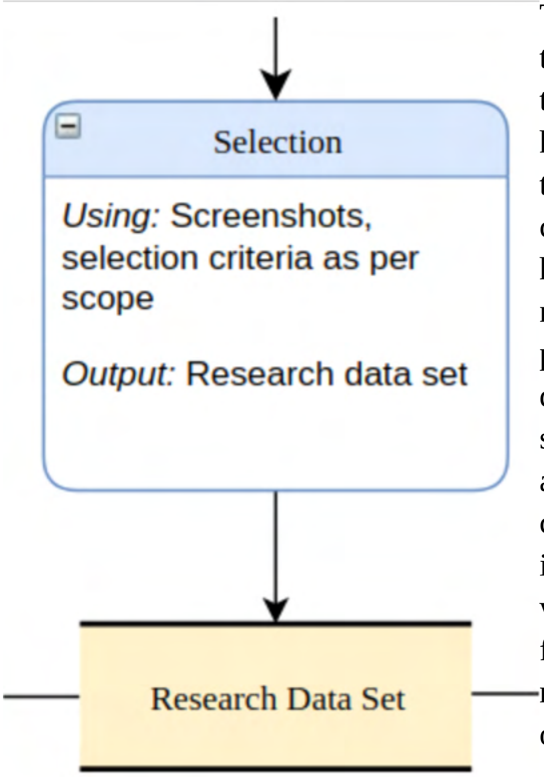

Selection
Using: Screenshots, selection criteria as per scope
Output: Research data set
Research Data Set

Figure 3.3: Workflow detail

As there is no metadata publicly available from which only political defacements could be identified, all saved pages had to be manually screened for suitability. As per the previously outlined definition, what is considered hacktivist in the context of the scope of this study is a conscious and deliberate injection (in the form of a defaced website) that is seeking deliberately to reshape public narrative. The criteria for a page to be in scope were, in short:

- A page must be political in the sense that is has a dedicated expression or argument of whatever quality.
- To qualify, a defacement must be situated between conventional and violent forms of protest. This is not to imply that hacktivism is a stepping stone, nor that hacktivism evolved from earlier forms of protest.

For the process of manually screening every single page, the screenshots proved to be very useful. With an image viewer software, a user can very quickly browse through a high number of images without having to wait for pages to load. In reference to the risk mitigation described earlier, screenshots are also a risk-free way of browsing cybercrime archives on any computer. In this initial screening, the table of saved pages was extended by another column. If a page was deemed to be in scope, the value “InScope” would be set to 1. This was enough for an initial screen and allowed for the browsing through of approximately 2000 pages in a day.

As the captured data was stored in batches of 1000 pages and screenshots, the next step in consolidating the dataset was to combine all pages that were deemed in scope. A script was used to carry out the following steps:

```
In every batch:
      Open the list of saved pages
            - Go through each line and check the
            “InScope” variable
            - If “InScope” is 1, copy the saved page and saved
            screenshot to the dataset.
            - Show the defacementID of the copied page
```

The final step then was to consolidate all lists from the batches and filter out only pages that were in scope.

During this process, a research diary was kept with entries on the kind of findings, general impressions and issues encountered. The main issues encountered while sighting and consolidating the dataset were as follows:

1. Sometimes pages were submitted to Zone-H, but they would either appear to have been restored already or to never have been hacked.
2. Sometimes pages would not load. This might be due to an administrator taking a hacked page offline.
3. Pages would use material (images and video) hosted on another server. Due to link rot, the majority of these materials are no longer available.
4. Some pages would only use images or videos, or they would feature an image of text rather than the text itself. Even if these pages still work properly, an automated text processing system cannot recognize this content. Optical character recognition (OCR) might be able to extract text from images, but only with varying accuracy. In most observed cases, images of text were used to display stylized banners and not to convey parts of the message.
5. A lot of material was in languages other than English or German, most notably Portuguese. With regards to the scope of this study, it was decided to only include English texts into the corpus. This decision will be limiting to the range and diversity of pages assessed, while enabling the use of automated text analysis such as tokenisation which would be distorted by a multilingual corpus.

   While it would have been possible to try and detect the language a defacement is in, and to attempt an automated translation, this would have meant that every translation would have to be checked for accuracy. These steps would have extended the scope of the study beyond its limits.

The first three points limited the usable number of pages in each batch as there were always a few pages that failed to load, or pages that relied on a 2nd party to host their content which has since removed the material or shutdown altogether.

The fifth point limits the amount of material that could be examined. Again, there is no way to pre-filter defacements and only select material of one specific language. The country flag, derived from the IP of the notifier, is no indicator of the language used in the defacement. In much of the older material, no IP has been recorded and no flag is present.

The output of this selection process is thus the research data set. In the next step, this dataset was moved into a database for automated analysis.

3.10.4 Filling the database

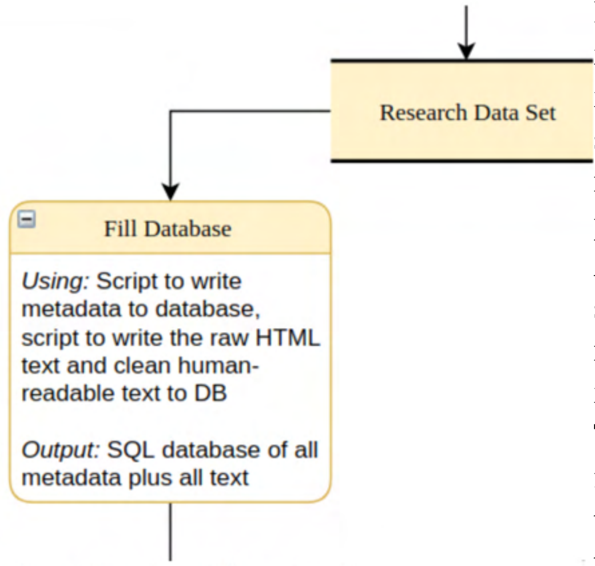

Research Data Set
Fill Database
Using: Script to write metadata to database, script to write the raw HTML text and clean human-readable text to DB
Output: SQL database of all metadata plus all text

Figure 3.4: Workflow detail

For automated analysis, the immediate crawler output of individual files and one metadata spreadsheet is not ideal. This is mainly because there currently is no place to store any analysis output. Another limitation is the lack of scalability of this model. It works reasonably well with >1000 files but is likely to hit limitations eventually. To enable analysis and to prepare for a possible future expansion of the collection size, the model was translated into a MySQL database with the following structure:

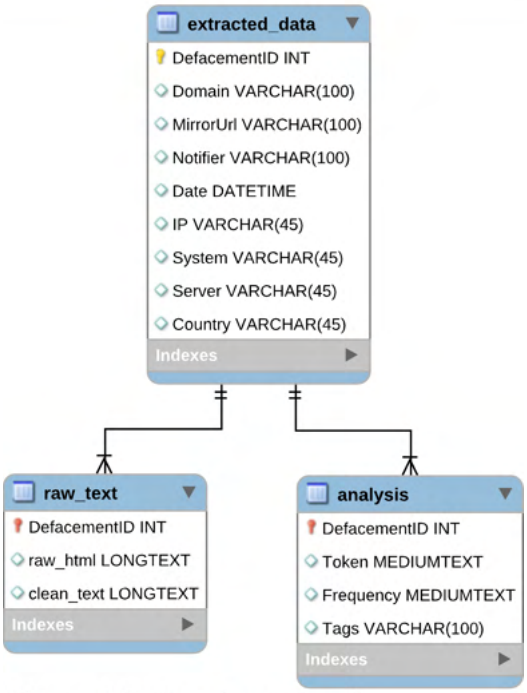


Figure 3.5: Database detail

All data extracted from Zone-H during the initial crawl was translated into a column in the extracted_data table. Two more tables were added. The raw_text table holds both the actual HTML of the scraped site as well as the pure text (with removed HTML tags). The analysis table at this stage is empty except for the DefacementId column. This table will hold the results of the analysis of individual files. In a later step, the individual results can be combined to analyse the whole dataset. This structure allows for greater scalability because, due to the performance of MySQL, it is less at risk of losing files or having them accidentally altered. The structure also facilitates a division between the scraped data, the extracted page content and the results of the analysis.

While it would be possible to store the screenshots in the database as well, it was decided to leave this for the archiving component of the project. The aim of the database is to allow for possible future extension and more convenient automated processing of the dataset. The screenshots are very handy for a human operator to sort through the pages and were essential for the creation of the dataset from the huge pile of scraped web pages but are not essential for text mining operations. Nevertheless, screenshots and the visual impressions of these defacements are a vital part of the data and will not be discarded.

Now that the database has been filled, the data is ready for analysis.

3.10.5 Metadata Analysis

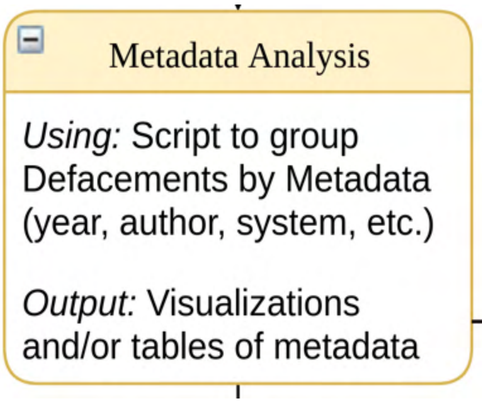

Metadata Analysis
Using: Script to group Defacements by Metadata (year, author, system, etc.)
Output: Visualizations and/or tables of metadata

Figure 3.6: Workflow detail

Agglomerating as a form of content analysis can be done using criteria derived from the page itself, such as time, date and location. Criteria may also come from the page's content, such as the presence of certain words or phrases, the use of images or embedded scripts. All the above criteria are suited for an automated analysis as they can be picked up by a search tool rather easily.

The idea of agglomerating data in such a way is to establish data on the prevalence of qualifying criteria in relation to time. Its result is the ability to make a qualified statement on the occurrence of a certain phenomenon over time. The implied claim of agglomeration is that the grouped together data share a common theme, and that its creators consciously chose said theme. This approach can be used to some extent to merge the attributes of selecting and contextualizing methods. Agglomeration selects, as it is a metadata-based approach, and is thus well suited for large amounts of data. The selection is in essence the reduction of the whole site onto one or a few selected criteria. The so collected metadata is then contextualized using spatial distribution, such as world map or a timeline. It is the relations between the data points in this spatial distribution, the vectors, which are then seen as the meaning-producing entity.

This conversion of spatial relations into meaning is what characterizes agglomeration as a medium between a relational, meaning-producing network as described earlier and a stringent narrative model of the past. In this medium role, the method of agglomeration can only partially fulfil the requirements of both models and any claims derived from it must always be critically inspected. This relationship between digital medium and content is described by Venturini et al.:

> Digital Methods can be defined as the repurposing of the inscriptions generated by digital media for the study of collective phenomena. The strength of these methods comes from their capacity to take advantage of the data and computational capacities of online platforms; their weakness comes from the difficulty to separate the phenomena that they investigate from the features of the media in which they manifest. (2018, 4195)

This difficulty is partially mitigated through understanding all hacktivist media manifestations as writing antagonistic text, as used in previous chapters. That approach expands the range of agency attributed to media. The benefits of that extended focus are described below:

> One trend we identify is a move to identify what are essentially 'literary' forms of criticality and suggest ways that they could be applied to the design of digital

> technologies understood as a process of ‘writing’. […] a focus on materiality (and its attendant philosophies) is attractive to RtD and DH researchers engaged with the building of artefacts because, at its best, it promises a fine-grained focus on what we can critically, theoretically, or philosophically say about what we are doing when we make things. (T. Schofield, Kirk, and Whitelaw 2017, 106)

The framing of the content analysis is thus exactly this tension between digital method’s struggle to identify the text from the medium and the material workaround of including both into an expanded notion of text.

3.10.6 Natural Language Processing

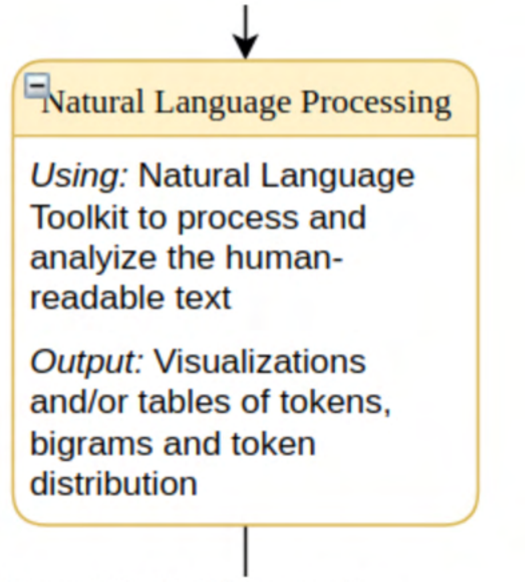

Natural Language Processing
Using: Natural Language Toolkit to process and analyze the human-readable text
Output: Visualizations and/or tables of tokens, bigrams and token distribution

Figure 3.7: Workflow detail

Further data analysis can be used to produce a quantitative overview of the dataset and provide justification for the selected case studies. The Natural Language Toolkit (NLTK) is a software platform for text processing in Python. It features a range of tools for the analysis of natural language text (Bird, Klein, and Loper 2009). NLTK is one of a range of similar software platforms, most notably StanfordNLP, OpenNLP, SpaCy and Gate (Schmitt et al. 2019). While these all share similar core functionalities, NLTK was chosen for the following reasons:

1. Accessibility and reproducibility

NLTK is an open source tool built for the open source programming language Python. This means that the entire workflow is build using freely accessible open source tools. Thus, replication of said workflow is possible without any restrictions in software access. This contributes to a transparent research design in line with FAIR data principles. It also allows for longevity of the research project as long-term usability of data formats is more likely with open data standards.

2. Documentation and reference availability.

NLTK is widely used for research in the humanities. There exists a body of literature guiding the use of NLTK for (digital) humanities research, such as Hofmann and Chisholm (2016) and Perkins (2010). Having that body of literature available helps to develop the workflow and learn the use of the toolkit. Since Python and NLTK are tools for this research, their use is utilitarian and driven by the pragmatic need for a reasonable automated text processing system.

3.10.7 Text mining

Text mining is commonly seen as a part of web scraping (Hofmann and Chisholm 2016, 106). It refers to the selection and agglomeration of relevant content to build a corpus. This may include, for example, the content of a tweet together with time, date and location, but not the replies or any other elements on the page. In this case, text mining starts with the archived pages in .txt format and is a twofold process.

The first step is to read whatever is stored in the raw_html column and strip away all HTML tags. This turns the content into pure text, omitting any content that can not be displayed.

raw_html	clean_text	HTML elements
<h1>Hello World</h1> <p>This is a sample paragraph</p> <img src = x></img>	Hello World This is a sample paragraph	<h1> <p> <img>

Table 3.7: Exemplified relation between HTML, human-readable text and HTML elements

As seen in the example in Table 3.7, all HTML tags have been removed leaving only the text. The image referenced in the raw_html section has also been removed. Naturally, a language processing workflow can only process natural language and needs to discard all artificial language elements such as HTML. Still, this means that information is limited and text displayed in images or videos is not added to the corpus. There is the option to reverse the progress and remove all content leaving only HTML tags behind. This could be used for a frequency analysis of HTML tags although this was not undertaken in this analysis.

3.10.8 Limitations of quantitative approach and DH condition

The process of text mining – that is the selection and consolidation of content for analysis – is dependent on stripping away from the source material all elements not deemed to be part of the natural language corpus. This is necessary for natural language processing, but it leads to decontextualization of the corpus as the natural language elements, the artificial language elements and design decisions produce meaning in their interplay rather than in isolation. For the quantitative analysis, a heading will be as important as text hidden in an HTML comment. This means that the note

```
<!-- Mirror of this Defacement provided by
http://defaced.alldas.de – >
```

has to be excluded from analysis since otherwise it would appear at the top of the token list since it is found in all earlier defacements. This is not unique to this study’s research objective but a common step in working with NLTK. Words to be excluded, so-called stop words, make up to 25% of a corpus depending on the type of source material (Bird, Klein, and Loper 2009). This means that not only the corpus used for quantitative analysis here is a piece of the whole with at least two other important meaning-producing elements missing, but also that the pure textual layer is reduced in size to make it accessible to a meaning-generating machine.

Natural language processing provides insight into common topics and phrases used throughout the research data set. It is a way of arranging individual pages into larger clusters of the same or similar topic. Further, it provides insight into the use of phrases and words over time.

3.10.9 Case study analysis

At this point, the file structure is as follows:

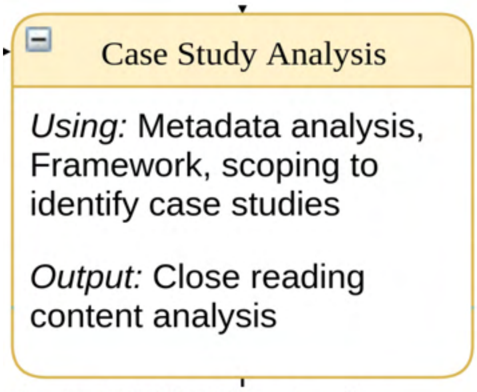

Case Study Analysis
Using: Metadata analysis, Framework, scoping to identify case studies
Output: Close reading content analysis

Figure 3.8: Workflow detail

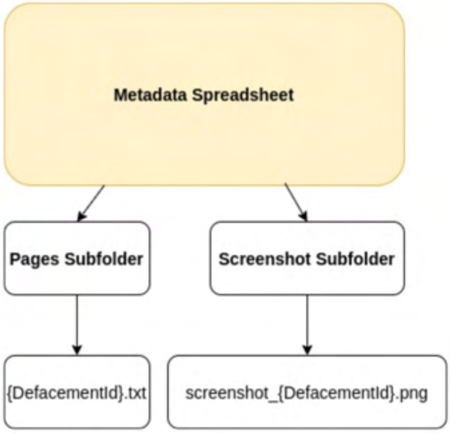


Figure 3.9: File Structure

The connecting attribute between the individual files is the unique DefacementId. This allows access to any saved page and saved screenshot. This structure is convenient because it allows the researcher to easily browse the dataset with common software. All is required is a file explorer, a simple notepad and image viewer software. This model allows for in-depth engagement with the defaced pages.

This step of the more manual side of the analysis was aided by findings from the analysis of the metadata which provided peaks in defacement activity and the findings from the NLP analysis which identified the key topics occurring throughout the data set.

3.10.10 Motivation and type analysis

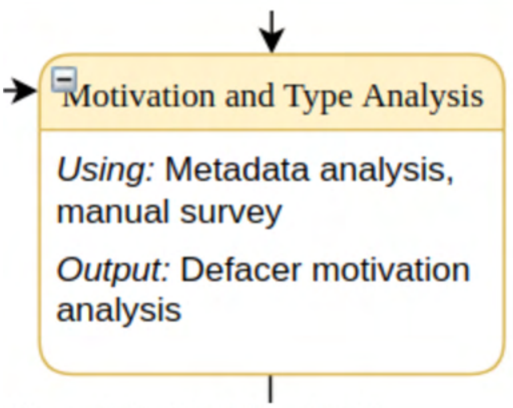

Motivation and Type Analysis
Using: Metadata analysis, manual survey
Output: Defacer motivation analysis

Figure 3.10: Workflow detail

Limiting data can be done through initial screening, such as that described briefly above and in more detail in the following chapter on the dataset. But the work of contextualization has yet to happen. Contextualization is the attempt to take the now limited data and expand it by connecting it to other data sets, such as geopolitical events over time. It is in the combination of the two research methods that I believe the most useful output can be achieved. Contextualization must be done with a proper theoretical framework to place the results in. It must be understood that web defacements a part of a hacktivist strategy are attempts to break into discourses, mostly through the use of visual material. Contextualization implies the virtual to be not a separate realm from the real, but an extension of it.

Richard Rogers advocates using the method of contextualization to avoid treating online environments like dreamworlds detached from reality:

> dispense with the idea of cyberspace and the virtual as primary points of departure for Internet-related research, or rather [...] reposition those terms to reflect the conceptual opportunities they currently offer. Cyberspace, with its origins in science fiction literature and its legacy in cybercultural studies, most recently has become a specific realm of inquiry in Internet security studies [...] Similarly, the virtual, a term with a rich theoretical history, refers less to the Internet generally than to virtual worlds such as Second Life and game environments such as World of Warcraft. Studies of the virtual, as in those specific types of online worlds and environments, would thus become a subset of Internet-related research just as cyberspace studies also now refers to niche areas: cyberwar together with cyberespionage and cybercrime. (2013, 203)

Roger's argument mentions the study of cybercrime which is positioned in the general realm of Internet-related research. The distinction between cyberspace and the Internet seems doubtful, especially in suggesting that anything "cyber" happens in a realm separate from the Internet. The conceptual opportunity lies in seeing cyberspace as a field worthwhile to engage in, as did hackers and hacktivists.

What is problematic with this concept is its implied notion of the cyberspace as a separate realm. This can lead to obstruction of the material conditions which brought about the idea of cyberspace in the first place. Contextualization must be carried out on the level of political economy of the medium itself before any content can be described adequately. Borrowed from the study of traditional media is this description of an approach to the political economy of media:

> [political economy of media] means investigating the nature of media ownership, how it is financed, the organisation of production and how this is regulated by

> governments and international governing bodies. This is important on the one hand simply to understand the nature of these organisations and processes, to know who controls our media. On the other it is at this level of analysis that we can find out why the content is the way it is. […] Such things cannot be understood at the level of textual analysis. (Hansen and Machin 2013, 32)

Adapting this to the study of hacktivist defacements means to look at the process of antagonistic writing described earlier. It is the question of who overwrites what that can hint at the organizations and processes at play. To understand why content is the way it is, the scope must be extended to also include technical limitations on what is possible within the medium and again what is possible within the context of a hacked site. The idea of media ownership is more complicated in this case. It might be argued that the very idea of defacing webpages is to utilize the relation between ownership and control (owner has no more influence over the page) and to finally invert it – the content now reflects (badly) on the owner of the page.

Contextualization must be carried out on a number of levels:

Temporal (metadata and dates referenced in source material)

As a first step, all pages must be contextualized regarding their time of occurrence as well as point in time referenced. This allows the positioning of any source material in a temporal context. It also allows estimation of the reaction time between any referenced event and its appearance on a hacked web page. The dates and events also offer an opportunity to group defacements.

Strategy and motivation

Strategy here means the description of the page's communicative function. For example, a page can be hacked to confront unsuspecting viewers with graphical content. It might also be argumentative, confronting unsuspecting viewers with a more or less coherent critical analysis. A page can also be in the tradition of adbusting – not overwriting but engaging with the original content of the page.

Strategy also applies to pages' relation to each other; they may be unique or they may be part of a series of identical pages. Either way, the strategy of dissemination can be put into relation to other pages. The way a page was hacked may be part of the communicative strategy – for example a difficult hack might show skills and be part of a message dedicated to a perceived enemy – as long as it is mentioned in relation to the hacktivist message.

References, both external (aimed at unsuspecting visitor) and internal (aimed at fellow hackers)

'References' is a subset of strategy; yet it deserves special attention. A reference can be many things, from a quotation to an actual hyperlink. What qualifies a reference in the context of analysing the source material is its communicative function. It must be assumed that this function can be fulfilled for the viewer. Those references mostly take the form of hashtags and links, as much as electronic communication is concerned, and the form of flags and other insignia otherwise.

This analysis is a form of discourse analysis attempting to reconstruct a discourse from fragmented evidence. Discourse analysis “draws on narrative theories that seek the underlying structures to look at activity sequences across different genres of communication and across different modes of communication.” (Hansen and Machin 2013, 172). All three described aspects – time, strategy and reference – are part of this discourse analysis.

Contextualization of the primary corpus through discourse analysis will be part of this study. The individual case studies using this method provide an in-depth look at material that the quantitative part of the analysis has confirmed to be emblematic for large clusters found within the dataset. It adds to the understanding of web defacements as a mode of political communication.

3.10.11 Long-term Storage

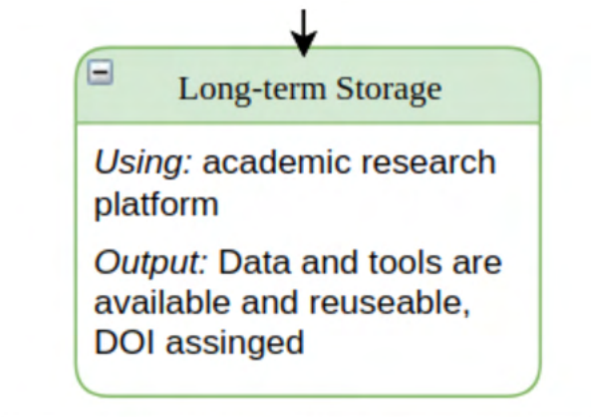

Long-term Storage
Using: academic research platform
Output: Data and tools are available and reuseable, DOI assinged

Figure 3.11: Workflow detail

Part of this research is not only to provide this study overview of web defacements from 1999 to 2002, but to make these defacements and the data derived from them available for further research. This is done in the light of the likelihood of more defacement archives disappearing and the existing collection being hard to access. The software and tools developed in the context of this thesis have also been preserved and are available under a permissive open source licence for future research to build upon. Outside the scope of this thesis is my project of building a web-based searchable interface for easy engagement with the existing corpus and other, similar material yet such a process would be part of a considered web archiving process.

The repository containing all self-developed programs is available online.

3.10.12 Data Output and Visualization

Part of the analysis of the data will involve visualizing findings so it is worth noting some issues in relation to that practice. For the data-based sections of the analysis, data from a variety of different sources is considered. The challenge this heterogeneous source material poses to data visualization, though, is to find suitable forms of representation. Data visualization describes the “visual representation of data and datasets which communicates precise information and values […] It is important, therefore, to consider data visualizations as objects for critical scrutiny, not just as mechanisms to communicate data” (Kennedy et al.

2016). Kennedy et al. acknowledge the need for research into how data visualization conveys meaning. A valuable extension of this debate is found in Streeb et al. (2019) where data visualization is seen as one aspect of a codification of real-world objects. This codification, the authors argue, is a transformation of entities:

> In comparison to the alphabet of all possible real-world objects and events, the alphabet of language entities is much smaller. So, the transformation from objects and events to language entities exhibits a huge amount of alphabet compression. Potential distortion is thus inevitable from time to time depending on the complexity of objects and events, the purposes of describing them, and the people who speak (write) and listen (read) (Streeb et al. 2019, 12)

Acknowledging a distortion in the representation of entities through any reference system, be it a natural or artificial language, is a perspective which allows to describe the limitations of a quantitative approach as a whole. What is often perceived as an inherent weakness of data visualization is the rhetoric of the visual, the selecting and ordering of data.

These shortcomings must be mitigated where possible. Regarding compression of alphabets especially in the visual, all data visualizations must be accompanied by a body of data from which they are derived. This will help to understand compression effects and lead to greater transparency in terms of selection criteria. All source material is released together with the visualizations.

Relating to the underlying problem of assuming meaningful output from an automated system working on codified entities[27], the increased reproducibility of NLTK and other open source systems might help to minimize the black box effect. Further, the functions used in this quantitative analysis are for the most part counting and accumulating functions of NLTK.

3.11 Concluding remarks on the chosen methodology

Throughout the design of this thesis, methodology has played a special role. This is due to the fact that while many of the steps described above are not new and untested methods in themselves, their combination with each other and with the research material has created new and sometimes unforeseen problems. To illustrate, web scraping is a well established method. Web scraping when the target site is severely restricting access required straying away from best practice and developing a custom scraping solution. A key aspect of this dissertation lies in the complex workarounds it has been required to develop and the method it has subsequently generated for capturing other ephemeral web data which is, as part of this thesis, now available under a permissive licence for public use.

[27] There exist multiple bodies of literature from multiple disciplines engaging with issues of codification of real-world objects and machine capacity to generate meaning. To mention just a few, see Berry (2014); Zuboff (2018); A. Galloway and Thacker (2007); Galloway (2015); Kirschenbaum (2012).

As seen in the workflow, the thesis is built on qualitative and quantitative analysis of the source material. This method will allow both a qualitative and quantitative analysis that ameliorates the limitations of each method – quantitative provides some certainty of representativeness both in that aspect of the analysis and in choosing case study examples – qualitative provides the rich contextual reading needed to access hacker culture.

It is, as the title says, a hacked-together approach. The following analysis chapters are built upon the data gathered from this process and will expand further on the respective parts of the method as necessary.

4. A quantitative dataset analysis

4.1 Introduction

This chapter provides a quantitative analysis of the dataset. The analysis in its first section will provide a set of formal criteria to distinguish web defacements used for political purposes from the general stream of hacked websites available on Zone-H. The collection of defaced pages at Zone-H is complemented by metadata about the attack such as time and date, attack method and defacer. For all defacements used in the context of this study, this metadata has been collected and aggregated to create a profile of political defacements. This profile can then be broken down to show the total defacements and active defacers per month.

In the second section of this chapter, the focus is shifted from an overview of the data available to a Natural Language Processing (NLP) driven analysis. This section includes common word occurrences, common word combinations and selected word frequencies distributed over time. The goal of this second part is to provide a quantitative overview of the entire dataset and also to serve as the basis on which a subsequent study, featuring a scaled number of web defacements can be placed.

This chapter provides the application of a framework for the analysis of web defacements as a whole, while it also argues for the clusters chosen for closer analysis – The Kashmir conflict and 9/11 – as both emblematic in their representation of web defacements and defacer communities. This argument is made by deducing the significance of both clusters from the available data. In analysing defacement numbers and active groups and tracing the use of different types of defacements over time, both parts of the analysis in this chapter root the selected clusters within the overall available data. This quantitative analysis clearly substantiates not only the importance of the two selected clusters within the overall dataset, it further shows the importance of certain high-impact defacer groups on which primary material is available. In laying the groundwork, this chapter thus serves a double function in that it provides arguments for the selection of individual examples and thematic collections to be investigated in more detail and that at the same time it also provides the methods for quantitative exploration of a larger dataset to identify thematic focal points for further analysis.

Hacker culture has its own lingo which can pose problems for analysis. As an example, think of the 7h3 pr4c71c3 0f 5ub5717u71n6 l3773r5 w17h 51m1l4r-l00k1n6 ch4r4c73r5 known as leet.[28] Add to this the fact that English proficiency varies greatly amongst defacers and that new expressions are being formed on the web faster than NLP libraries can incorporate them. Literature addressing this

[28] Decode at http://www.robertecker.com/hp/research/leet-converter.php?lang=en Also see Grabbe (2016).

condition of non-standard use of language on the Internet (Zupan, Ljubešić, and Erjavec 2019; Sreelakshmi, Premjith, and Soman 2020) exists, but no works specific to the NLP-based analysis of defaced web pages have been published to date.[29] While it would be possible to change most of the non-standard expressions into regular English expressions, this would come at the cost of further losing accuracy in analysis. For the purpose of this quantitative analysis, which is to provide an overview of the entire dataset and to substantiate the reasons for selecting individual case studies, NLP was employed only insofar as it contributed to this goal.

4.2 The Problem of Data Visualization

This chapter features a range of different visualizations for metadata and defacer motivation. These different visualizations have been chosen to best reflect the underlying data. Some are common forms of data visualization such as bar charts while some are less common forms such as radial charts or stacked charts. The decision to use either of these forms was driven by the number and nature of data series for each visualization.

As an example, a plain bar chart visualization takes two data series (x and y, or defacements and time) and its visualization suggests a correlation between the two. Bar charts can be expanded by combining multiple bar charts that share the same y variable such as multiple tokens over time. This is useful and a number of bar chart and line chart visualizations are used throughout this chapter, however there are limitations to this form of visualization. The first is a practical consideration; more data series make visualizations harder to read. As a solution, in some cases bar charts can be stacked to show both the total count of a data series as well as its constituent sub series. This is the case in the defacer groups over time visualization (Figure 4.3 and 4.4). In other cases, it can be useful to merge bar charts into a radial chart as seen in Figure 5.1. This results in a visualization resembling a profile and allows quick comparison to another profile. Using words such as comparison already hints at viewer interpretation, arguably the key feature in data visualization, yet interpretation is more easily misguided in data visualization than in textual or numerical presentation. Touching only superficially on theories of visual perception here, it should be assumed that every part of a visualization will be interpreted. Proximity and similarity of elements will increase this tendency (Wong 2010).

Whatever appears on the screen together, is likely to be interpreted as having some relation. Keeping in mind that all elements of a data visualization are likely to be read as being related to each other, whenever different data series are shown, their relations must be considered. This means that in a "top tokens per year"

[29] An article describing the practice of using defacer names including all non-standard spelling to trace defacers across collections has been published by the researcher. See Kurzmeier (2020).

visualization (Figure 4.11), the data series cannot be presented as mere token count, but must be further abstracted into token frequency so that the individual data series are comparable. A similar approach is taken in the case of Figure 4.12, where all values are represented as percentages of the total, so that a comparative interpretation of the neighbouring bars is possible.

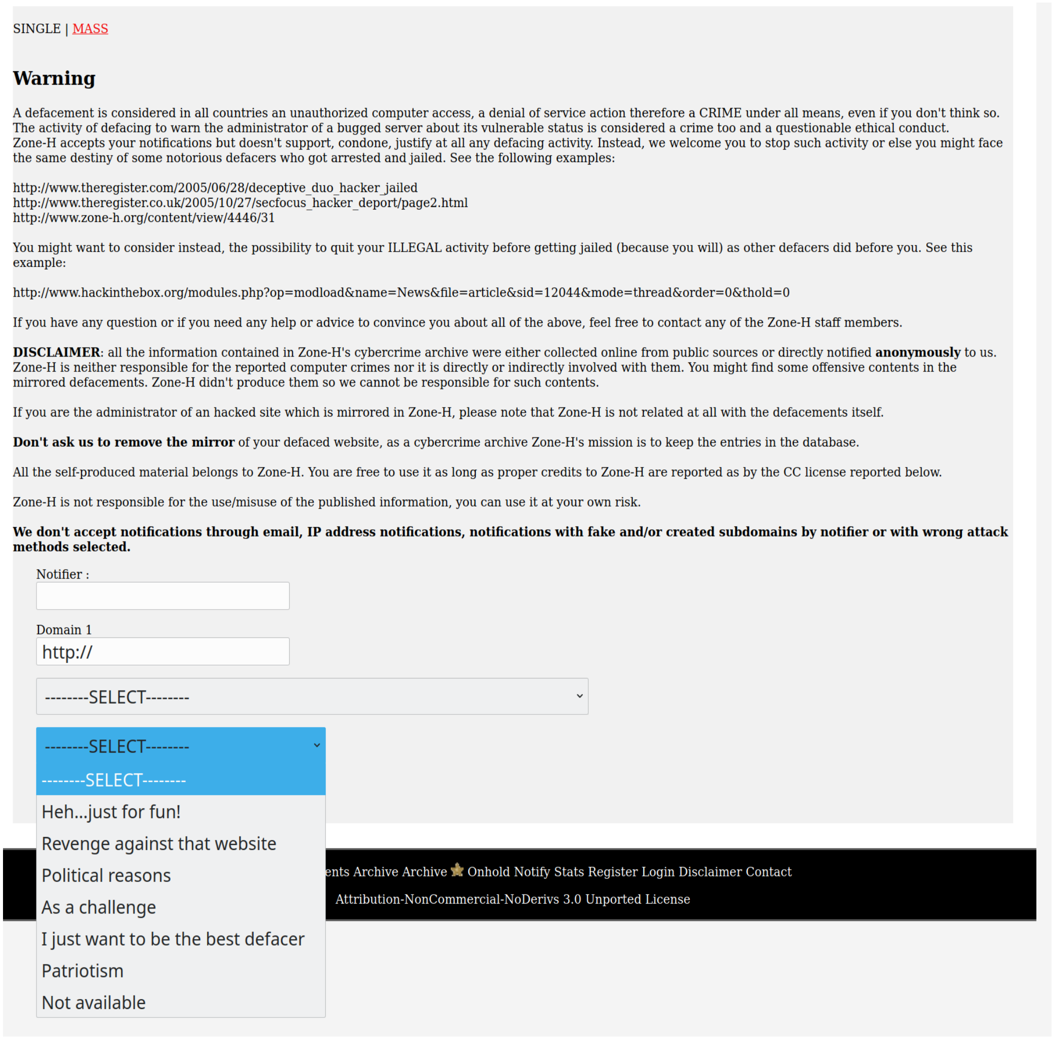
In summary, the choice of visualization types was mainly driven by this consideration: the need to express more than two data series (such as combinations of ends-oriented and expressive incentives such as in, Figure 4.15) in such a way that allows comparison across all elements of the visualization by either providing a breakdown of the total or expressing the data as a fraction or frequency of the total.

4.3 A qualitative exploration of metadata

4.3.1 Overview

Metadata on defacements held in the Zone-H collection is created in two separate steps. When submitting a defaced page, the notifier has to give the name of the attacker and the URL of the defaced page. The attacker name can be chosen at will, but in practice is always the alias of the defacer. Additionally, from two menus the notifier has to select the attack method and motivation for the attack. Both fields do not allow free text entry and even though it is stated that no notifications with the wrong attack methods will be approved for inclusion in the collection, this is practically impossible to verify. Whatever the user input here, only the alias (named notifier in the below screenshot) and the URL will become part of the metadata associated with the archived defacement. Users do not need to be a registered member of the community to report pages; the form is open to anyone. Selections from the two drop-down menus are aggregated into yearly statistics and it is not possible to filter pages by motivation or attack method.

The structure of this submission page strongly shows how Zone-H is built around the defacer themselves submitting the defaced page to the archive. Not only are all fields mandatory, but the field “reasons for defacement” refers to author’s or perpetrator’s knowledge and may in most cases only be correctly answered by the original author.



SINGLE | MASS

Warning

A defacement is considered in all countries an unauthorized computer access, a denial of service action therefore a CRIME under all means, even if you don't think so.
The activity of defacing to warn the administrator of a bugged server about its vulnerable status is considered a crime too and a questionable ethical conduct.
Zone-H accepts your notifications but doesn't support, condone, justify at all any defacing activity. Instead, we welcome you to stop such activity or else you might face the same destiny of some notorious defacers who got arrested and jailed. See the following examples:

http://www.theregister.com/2005/06/28/deceptive_duo_hacker_jailed
http://www.theregister.co.uk/2005/10/27/secfocus_hacker_deport/page2.html
http://www.zone-h.org/content/view/4446/31

You might want to consider instead, the possibility to quit your ILLEGAL activity before getting jailed (because you will) as other defacers did before you. See this example:

http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=12044&mode=thread&order=0&thold=0

If you have any question or if you need any help or advice to convince you about all of the above, feel free to contact any of the Zone-H staff members.

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents.

If you are the administrator of an hacked site which is mirrored in Zone-H, please note that Zone-H is not related at all with the defacements itself.

Don't ask us to remove the mirror of your defaced website, as a cybercrime archive Zone-H's mission is to keep the entries in the database.

All the self-produced material belongs to Zone-H. You are free to use it as long as proper credits to Zone-H are reported as by the CC license reported below.

Zone-H is not responsible for the use/misuse of the published information, you can use it at your own risk.

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Notifier :

Domain 1
http://

--------SELECT--------

--------SELECT--------

--------SELECT--------
Heh...just for fun!
Revenge against that website
Political reasons
As a challenge
I just want to be the best defacer
Patriotism
Not available
ents Archive Archive Onhold Notify Stats Register Login Disclaimer Contact
Attribution-NonCommercial-NoDerivs 3.0 Unported License

Figure 4.1: Submission form for new defacements on Zone-H.

The open drop-down menu shows the possible answers for "reasons for defacement"

Once a defacement is processed by Zone-H's web crawler, a second set of metadata is created automatically. This includes the time and date of the capture (not the attack), the system the target page was running on, the web server software, and the IP address of the target if available. In cases where the target IP address can be associated with a country, the respective flag is shown.

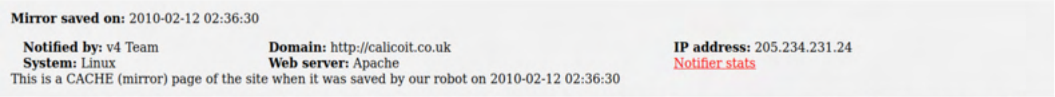
Both sets of metadata are then combined and are shown in the header of an archived page. The header contains the following elements taken from the submission form:

- Notifier
- Domain

And the following elements provided by the crawler:

- Timestamp of capture

- System
- Web Server
- IP address



Mirror saved on: 2010-02-12 02:36:30

Notified by: v4 Team **Domain:** http://calicoit.co.uk **IP address:** 205.234.231.24
System: Linux **Web server:** Apache Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2010-02-12 02:36:30

Figure 4.2: Header of an archived defacement showing automatically extracted metadata.

An IP address has been recorded, but no country flag has been assigned.

4.3.2 Trustworthiness

There are many reasons that this dataset may be unreliable. Notifier, motivation and attack method can be forged at will, and there is no realistic possibility Zone-H's volunteers could check every single one of the hundreds of thousands of submissions. The URL could be forged, although this would cause the crawl to fail and the page not to be archived. The IP address is that of the attacked server, not the notifier. It must be legitimate for the crawler to run, but is only interesting for the analysis where it can be translated into a location.

The timestamp is extracted on the crawler side and canot be manipulated by the notifier. There has been no considerable delay recorded between notification and capture, so that from here on, the capture date will be seen as the defacement date. The remaining elements, listed below, are provided by the target system and can also not be manipulated by the notifier:

- System
- Web server
- IP address

These components of the entry can, however, be manipulated by the defaced system as part of a security mechanism. As good security practice, a web server should not answer queries unrelated to its purpose, meaning that a server hosting a web page has no reason to disclose its operating system and version. In addition to that, depending on the attack method, an attacker could completely take control of a target system and eventually manipulate the metadata provided by the target system, possibly with the intention to make the attack seem harder and thus more prestigious than it actually was. Although no case of this practice has been observed, it must be considered when discussing the metadata.

Relating to a description of metadata trustworthiness in relation to defaced pages by Maggi et al., the following assessment is made of the available Zone-H metadata:

Attribute	Example	Description	Trustworthiness	Explanation
Domain	http://calicoit.co.uk	URL of defaced page	High	Must be correct for site to be archived.
Timestamp	2010-02-12 02:36:30	Timestamp of mirroring	High	Provided by the crawler, not the notifier.
System	Linux	The operating system of the defaced page	Low	It is good practice for a server to not disclose this information. May also be forged by attacker.
Web Server	Apache	The server software at the time of attack	Low	It is good practice for a server to not disclose this information. May also be forged by attacker.
IP Address	205.234.231.24	The IP address of the server	Medium	Derived from URL, can be obscured through proxy.
Notifier	Gforce	Name of the person notifying Zone-H of the defacement. Usually synonymous with the attacker.	High	Defacers submit for exposure and have little reason not to claim recognition for their work.
Motivation	Political Reasons	Motivation for the attack	Low	Pre-defined answers, attacker has no gain in answering truthfully.
Attack Method	SQL Injection	Method for the attack	Low	Pre-defined answers, attacker has no gain in answering truthfully.

Table 4.1: Assessment of defacement metadata, based on Maggi (2018)

Assessment of trustworthiness varies since some defacement collections (used to) rely solely on user input to create metadata. However, the general direction is to regard as trustworthy only those elements of metadata which are either necessary for the crawl to run successfully or that are created automatically during the crawl. The following metadata analysis will thus be based on the values which are present in the header as shown in Figure 4.2:

- Domain (URL)
- System
- Web Server
- IP Address
- Notifier

Following on from methodological considerations, the following sections will present the available data in detail. Their general order is to start with concrete and highly reliable metadata such as time and domain and continue on to less tangible data such as motivation.

4.3.3 Distribution over time

The following graph shows the distribution of in-scope defacements over time grouped by month:

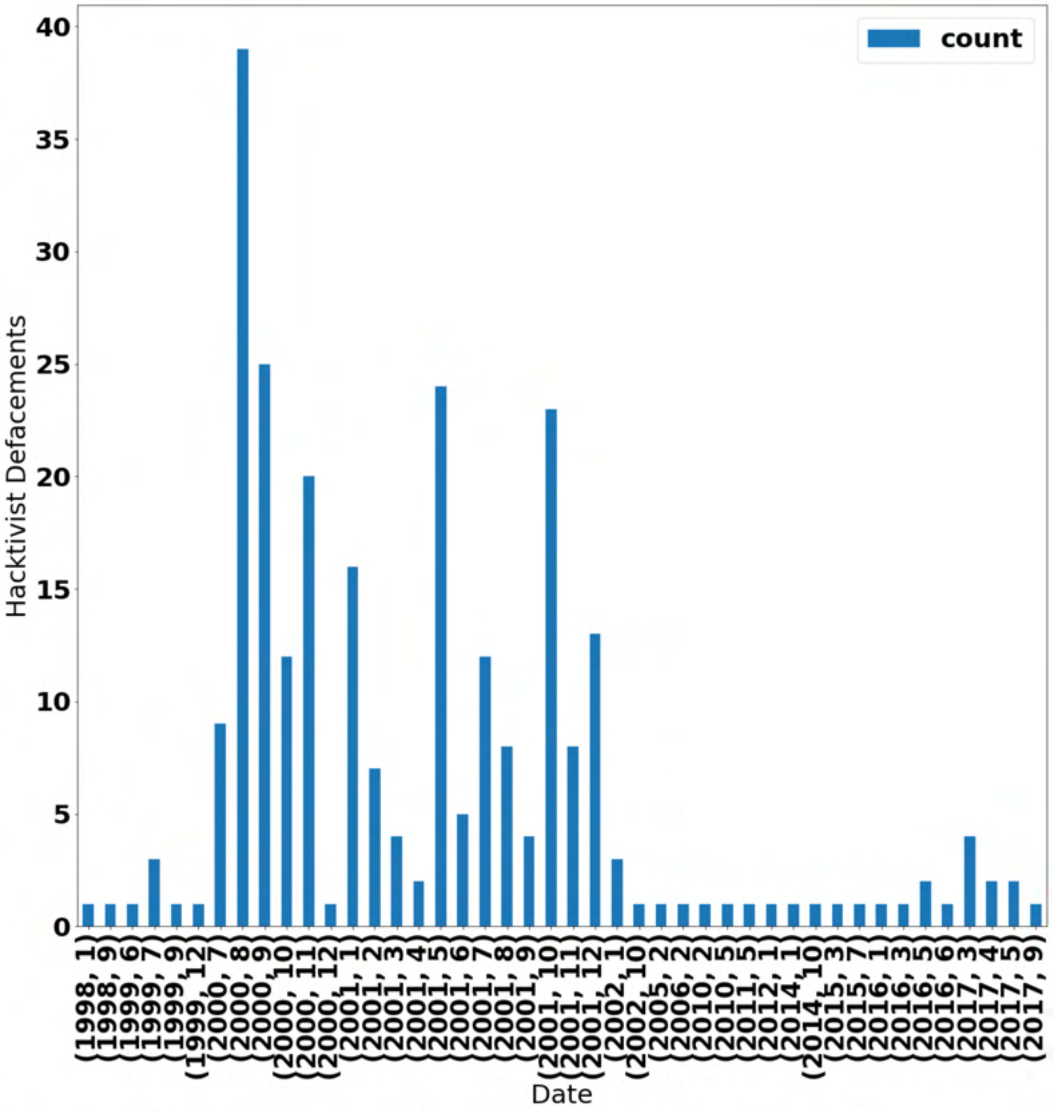


Figure 4.3: Distribution of defacements over time, grouped by month

Months without captured defacements are omitted in this figure. The results show two periods of high defacement activity, one around August of 2000 and another one between May 2005 and December 2001. As will be shown in more detail in the following, these two spikes represent defacements around the Kashmir conflict and 9/11. Even looking at this purely numerical representation of attacks, the influence of real-world events on defacements is shown. This observation supports the assumption that web defacements may be triggered by geopolitical events and that defacers act in coordinated campaigns. This is supported by findings by Balduzzi et al. who in a large-scale study on the threat to cybersecurity posed by defacements found that:

> [m]ass attacks, or attacks that typically use automated hacking tools to compromise as many websites as possible indiscriminately, are common across the web. But in the course of our research, we noted a more coordinated form of attack that we labeled “campaigns”. In a campaign, the attackers launch specific attacks as a reaction to certain events, to push an agenda, make known their grievances, or spread political messages. (Balduzzi et al. 2018, 11)

Although working on a different set of defaced pages and having a broader scope than this study of defacements, Balduzzi et al. nevertheless find the Kashmir conflict to have produced the largest number of defaced web pages (ibid).

The distribution over time serves as an introduction to the quantitative study of metadata, as it provides a first overview of the available data and already hints at the geopolitical events which may have caused the surge in defacements. Approaching this data with the theory that web political defacements are caused by geopolitical developments allows us to deduce thematic focal points which are likely to be found in a collection. Distribution over time relies on a somewhat evenly distributed coverage of the time period in question and can be an effective tool for internal comparison of the dataset. However, such a material-over-time analysis must always be seen in the light of the collection practice. As sources pre-2000 are generally scarce, and the post-2002 era is only covered by 2000 randomly selected defacements, comparing these results to overall web defacement activity is difficult. In the next step, this data will be contextualized to trace defacers and defacer groups over time.

4.3.4 Active defacers over time

If the above distribution over time is a high-level indicator of the overall defacement activity recorded by Zone-H during a certain time, the following breakdown of active defacers over time provides a more close-up look on that data and adds another layer of information, showing defacer diversity for a given time period and visualizing the lifespan of some of the most influential defacer groups in the dataset.

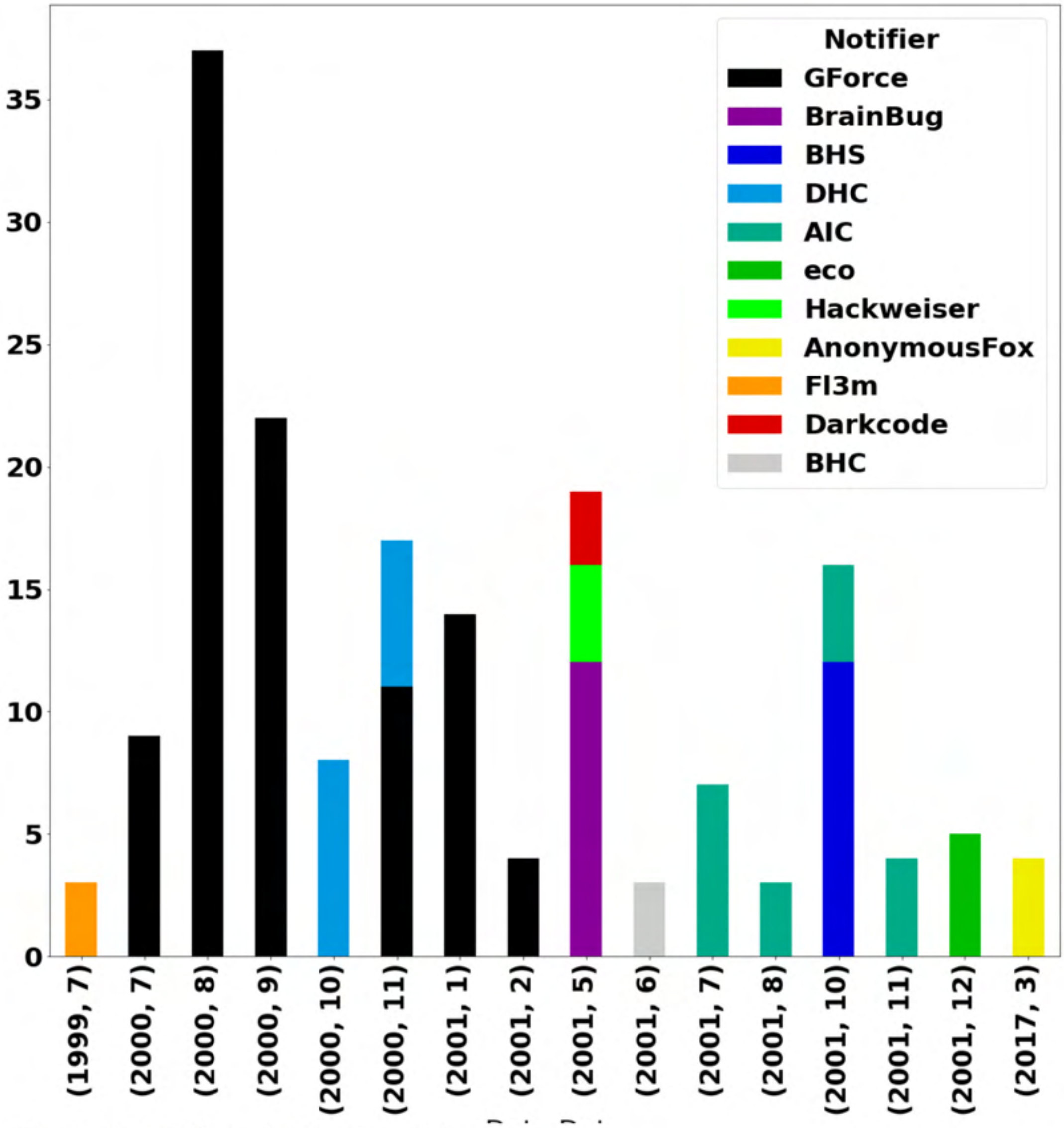


Figure 4.4: Selected defacer activity over time

Figure 4.4 shows active defacers per month, focussed on months with more than one active defacer and only showing the overall top defacers by volume. In the centre again are the two peaks of August of 2000, May of 2001 and October of 2001, similar to how they appear in Figure 4.3. The visualization us allows to quickly see how the first peak between July and September of 2000 was due to very high activity by GForce, while the second peak between August and October of 2001 was caused by defacements submitted by AIC, BrainBug and BHS.

Drawing from the information provided here, primary material was sought on these very active groups, which was successful in the case of Gforce and AIC (both active in the context of the Kashmir conflict) as well as BHS (later active in the context of 9/11). The value of the above visualization is thus not only to sort defacers by number of pages attacked, but also to see their longevity and identify worthwhile subjects for further research. It is from such a reconstruction of the significance of certain defacer groups within the scene at the time that the analysis of material such as interviews and defacer's own homepages becomes embedded in their historical context.

It is further interesting to see the rather short life spans of defacement groups. GForce and AIC both submitted political defacements for five to six months, while most other names only appear in one or two months. The existence of thematically focussed groups defacing pages in coordination as the standard operating mode for defacers aligns with the finding that:

> [e]specially if driven by strong ideologies, defacers are not lone wolves, but their modus operandi resemble that of well-organized cyber gangs acting in a coordinated fashion. After manually inspecting several thousands of deface pages, we confirm that modern defacers tend to be affiliated in teams and by no means act as "script kiddies". (Maggi et al. 2018, 446)

It is entirely possible, and in fact hinted at in some of the names such as AIC (Anti-India-Crew), that groups are following ideologies and might be formed for one specific purpose while the individual members continue hacking long after a group has ceased to deface pages. This explains why some groups – focussed on an ongoing conflict such as GForce – submitted defacements for such a long time while the events of 9/11 sparked a comparatively small but diverse set of defacements. Looking at groups not as a place where defacers start out, but where established hackers convene to work together, the rapid speed with which groups put themselves on the charts is explained. Defacement groups are where skills are applied and ideology is already agreed upon, the first being part of the admission criteria and the latter being a small piece of common ground to base the communal work upon.

The data analysed in this section challenges the idea that hackers primarily act as individuals, or that they tend to be organized in tight-knit, persistent teams. Rather, the most influential defacers work in fluid groups with a short lifespan but a high degree of focus. These groups are formed around a common cause or issue and are driven by effectiveness. The data analysis further showed that because of the team being the default mode of defacer organization, this breakdown of active defacers over time is well suited to identify relevant groups, especially since this method can be scaled to survey a much larger dataset.

The communal work leaves traces in the affected systems, some of these traces are recorded in the form of metadata relating to the hacked systems. In the following, the metadata which was captured during Zone-H's collection process will be analysed.

4.3.5 Top-Level-Domains (TLDs) attacked

The following five sections on TLDs, location, server types and operating systems are generally concerned with profiling political web defacements and contrasting said profile against the backdrop of Zone-H's overall collection. This is done to compare political web defacement's metadata against all available metadata with the intention to potentially identify political web defacements through their metadata profile. Further, this effort aims to answer the question of quantity or quality being the focus of political defacer's efforts. In other words, do political web defacements generally prefer high-value targets at the cost of reduced quantity, or do they prefer to deface as many pages as possible?

A TLD is part of a web page URL and represents the highest level of the Domain Name System of the Internet (Postel 1994). TLDs can be restricted politically (such as .ie for Ireland), organisationally such as .edu for pages associated with higher-level education in the USA, or be generic and readily available such as the .com domain. Important for the context of this study is that since TLDs can give an indication of where the target is located (in the case of country-coded TLDs) or even what organisational affiliation the target had (for example .edu or .mil for, respectively, 3rd-level educational facilities and US military sites). TLDs are managed by a range of authorities and while some have disappeared from the web, others have been added (Wikipedia provides a comprehensive list of TLDs). As TLDs are managed by a range of authorities, there are a range of rules regarding TLD allocation. As an example, to receive a .US domain, the applicant must be:

> 1.A natural person (i) who is a United States citizen, (ii) who is a permanent resident of the United States of America or any of its possessions or territories, or (iii) whose primary place of domicile is in the United States of America or any of its possessions [...],
>
> 2.A United States entity or organization that is (i) incorporated within one of the fifty (50) U.S. states, the District of Columbia, or any of the United States possessions or territories, or (ii) organized or otherwise constituted under the laws of a state of the United States of America, the District of Columbia or any of its possessions or territories (including a federal, state, or local government of the United States or a political subdivision thereof, and non-commercial organizations based in the United States) [...] or
>
> 3.A foreign entity or organization that has a bona fide presence in the United States of America or any of its possessions or territories … (usTLD n.d.)

It is easy to image how this system can be circumvented by providing false information or having a US citizen register the domain for a foreign applicant. The point to make here is that a TLD is a good indicator of the image and association of a web page, but it is not a highly reliable source of national attribution.

The following figure gives an overview of all attacked TLDs as they were submitted to Zone-H's crawler. Direct links to .html files were discarded.

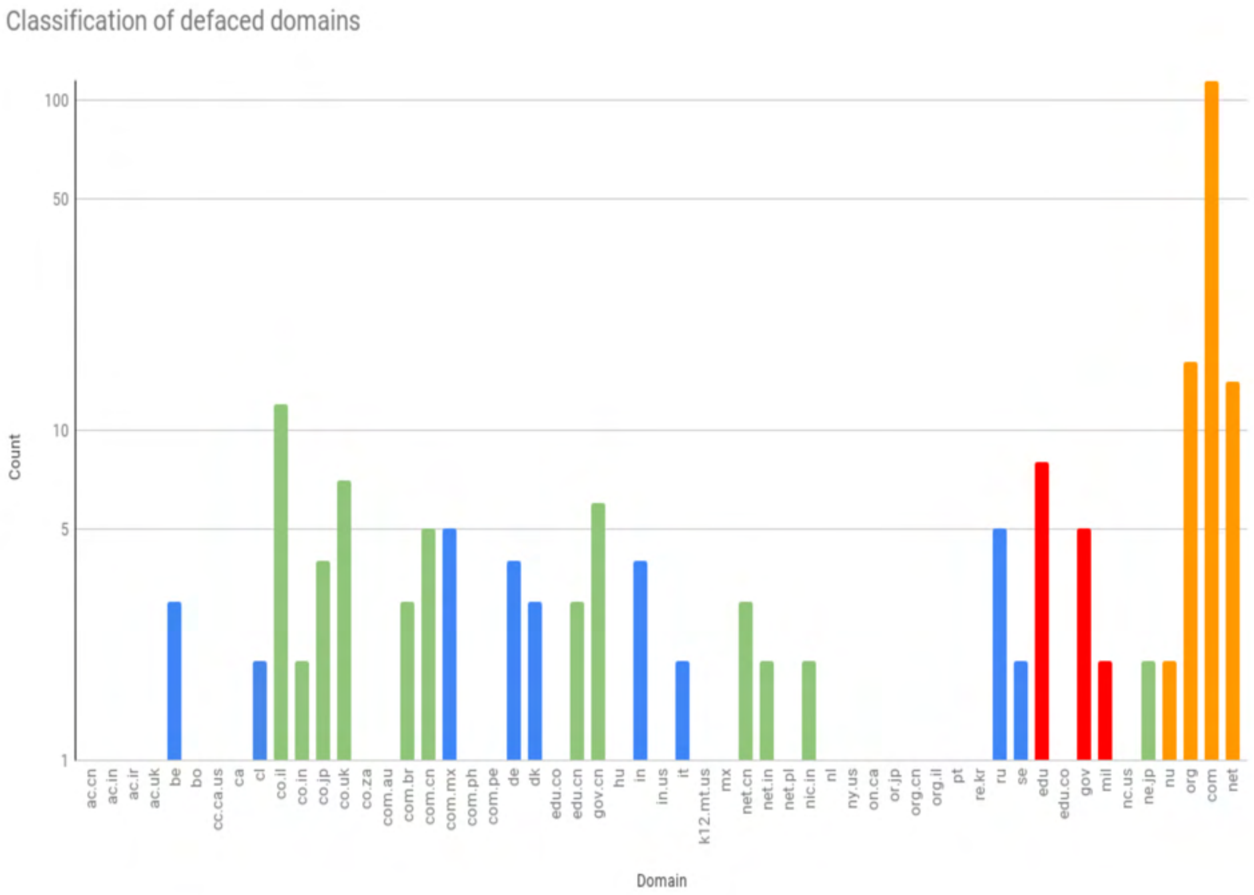


Figure 4.5: Totals of all TLDs defaced, logarithmic scaling

Generic domains in orange, institutional domains in red, geographic domains in blue. Mixed types in light green.

The findings show that the generic TLDs .com, .net and .org make up the largest share of all defaced pages. This is followed by a range of more specific TLDs such as .edu, .gov as well as some "preferred" national TLDs .de (Germany), .ru (Russia) and .in (India). The results from this TLD analysis can mainly be used to compare the target selection of defacer groups across different campaigns. This more detailed look at defaced TLDs will play an important part in the analysis of 9/11-related defacements (see Chapter 6).

General assumptions which can be drawn from this are that while generic TLDs are the most common form of TLDs found, defacers also target specific domains such as .edu and .gov. Maggi et al. in a broader study of web defacements came to similar results and suggest a division between targeted and opportunistic attacks:

> the top TLDs are .com.br (4%), .de (3.5%), .co.uk (3.2%), .nl (2.5%), .it (2.3%), and .ru (2.2%). [...] Note that, the choice of the target could be guided by the type of message (e.g., attacking a national or .gov website to protest against the government), or simply by chance (e.g., small websites are more vulnerable). Indeed, most of the targets are popular web applications (WordPress, Joomla, and Drupal), frequently targeted by automated exploitation scripts whenever a new vulnerability is found. (Maggi et al. 2018, 445–46)

Maggi et al.'s regarding TLD distribution are in line with my own observations from the research data set. The division between more vulnerable and more prestigious targets is a frequent topic of scene-internal debate and many of the hacker to hacker elements of communication described later on address this. The observation that defacers may use automated tools to deface all sites with known vulnerabilities is important throughout the following case studies as it leads into a quality versus quantity discussion when it comes to target selection[30]. As Zone-H only refers to the total number of defaced pages to create the "most active notifier" list, it is reasonable to assume that quantity plays an important role for many defacers. The discussion in relation to web defacements as tools in political communication revolves around whether it is possible to show that groups also target specific sites because they are high-value targets. As one of the defacer groups, AIC, has been active in both the Kashmir and 9/11 cluster, it is possible to compare the attacked TLDs to further investigate the existence of an active target selection process.

[30] In 2013, close to the time period analysed here, over 42.000 of the Internet's top one million sites were running on Wordpress, of which 73.2% had known vulnerabilities (Abela 2020). With little effort, a defacer can automatically attack and submit thousands of defacements based on these low-hanging fruits.

4.3.6 Locations

Most ip4-addresses can roughly be translated into a location. Zone-H records this IP address when the crawler accesses a server to take a snapshot of a defaced page. This is then used to show the respective national flag of the country the server is physically located in. However, this data is problematic for the following reasons:

1. Zone-H has incorporated a lot of older material from now defunct site alldas.de. Alldas did not record the IP address and thus no location is available for these defacements.
2. If a page is hosted by a hosting provider, it might not even be clear to the website owner where the data is physically located. For example, an Irish (.ie) website might be hosted on US servers and thus appear as an US flag.
3. For security purposes, a server might not allow direct connections but make us of a middleman, or reverse proxy. This then obscures the actual IP address.

Those caveats aside, the following graph shows the deduced location by IP address:

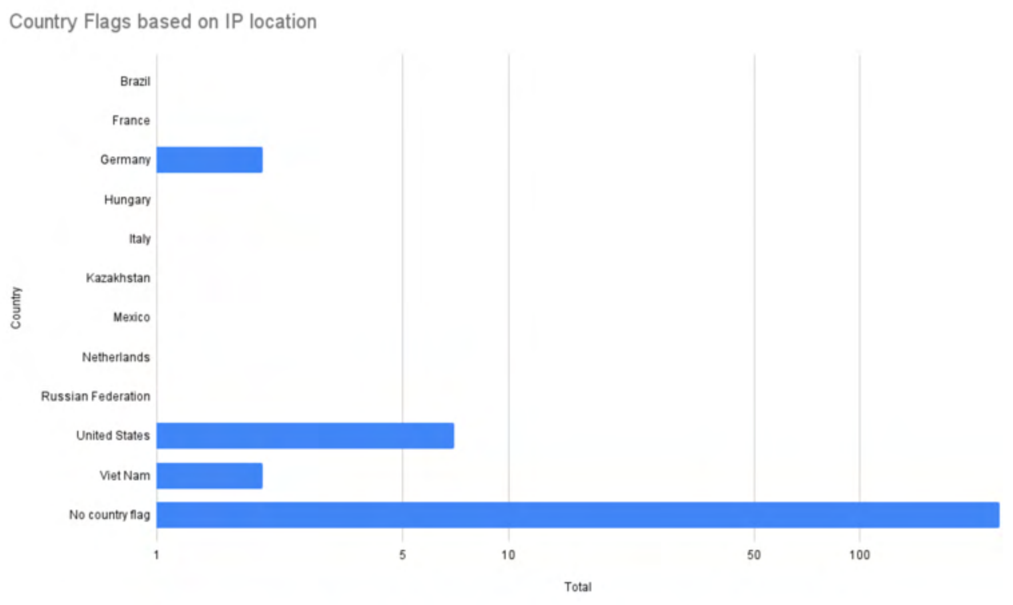


Figure 4.6: Country Flags based on IP location, logarithmic scaling

The numbers show how for most defacements, no location could be determined. The most numerous location was the United States, followed by Germany and Vietnam. Translated onto a map, the distribution looks as follows:

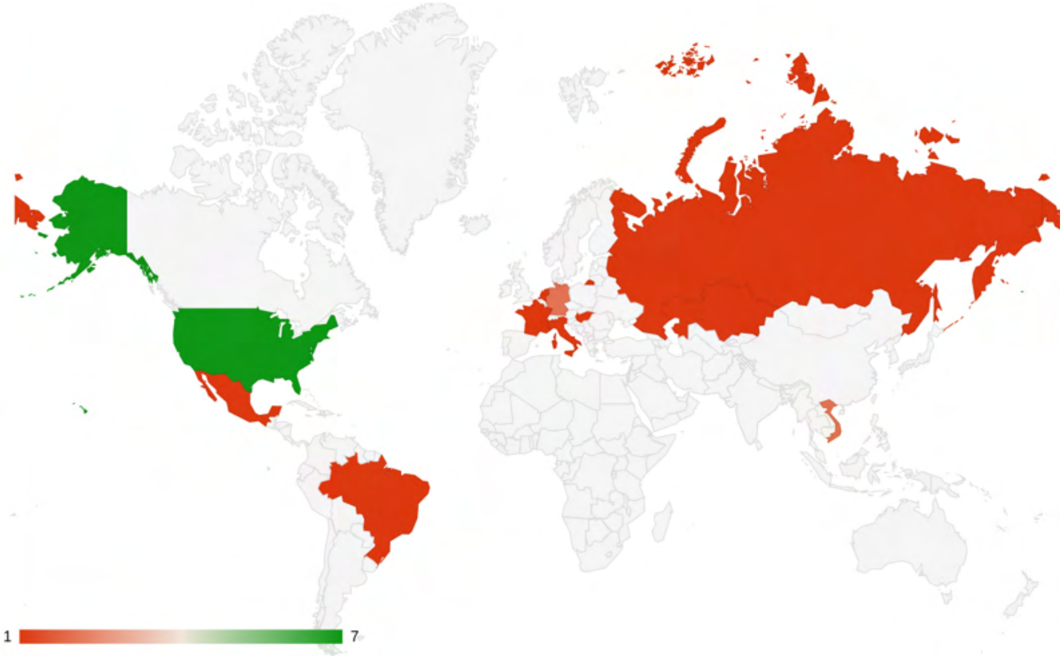


Figure 4.7: Heatmap of attacked sites

Comparing these results to the previous analysis of TLDs shows that the very high number of generic domains defaced such as .com, .net and .org finds its representation in the US as the most affected region. Brazil, with an active hacking community, finds only one mention. Most likely due to the German focus of alldas.de, German servers also show as one of the top locations. Surprisingly, Russia and Vietnam, two regions hardly, if ever, mentioned in defacements, also feature on the map. These regions might simply be the location of inexpensive data centres hosting various pages.

The high discrepancy between the affected TLDs and the actual location of servers is likely due to the reasons described above. There is generally little correlation between the events and the server locations. The Kashmir conflict, around which a large cluster of defacements exists, has not led to one Pakistani or Indian server being affected. If anything can be deduced from this small and incomplete sample of IP-based locations, it is that defacers follow their (target) audience more than their targets. This means that more focus seems to have been put on reaching a Western audience than attacking servers of a perceived enemy nation.

The discrepancy between targets, infrastructure and audience also serves as a reminder of the different layers of the Internet. TCP/IP, the protocol which facilitates most communication between computers browsing the web, is described by four distinct layers. In a simplified overview, these are[31]:

- Link, managing the physical interface
- Internet, managing the connection with other devices

[31] Hereby following RFC 1122 for layer count and naming. For further information beyond the scope of this study, see Sunshine (1989); Network Working Group (1989).

- Transport, managing the transport of data
- Application, enabling applications to send and receive data over the network

These four layers build into each other, with Link being the most physical and Application being the most abstract. Web defacements generally affect the Application layer (displaying the defaced page) and attack methods might affect both Application and Transport layer.

Similarly to these TCP/IP layers, the Internet on a larger scale can also be described as layered, building on a physical architecture of wires and magnetic disks and leading up to the appearance of a website in a browser. Again, web defacements are a phenomenon of the higher, more abstract levels while cyberterrorism and -warfare can be classified as aimed at the more physical layers. Diving down to the IP addresses and translating the abstract URLs into the physical address of a machine providing the .html document to a browser is the attempt to translate web defacements from their original, abstract and high-level down to the physical infrastructure of the web. This attempt is useful for the analysis as it reveals more about who defacers are, what they understand their audience to be and whether their campaigns are more of a representation-focussed digital iconoclasm or more of an infrastructure-focussed blockade.

4.3.7 Operating System and Server Software

During the crawl, information about the defaced server was gathered automatically and added to the metadata. The data relevant for this section will be the operating system and the server software detected. While Maggi et al. describe the trustworthiness of the server software as low, they nevertheless acknowledge a general alignment between their data and usage statistics (2018, 446). In the case of Zone-H, the data about the server must be generated automatically by the crawler as it is not recorded on the submission form. While this speaks against deliberate falsification by the notifier, as has already been indicated, it is still good security practice for a server to not disclose its operating system and server software to visitors.[32] For this reason, the operating system and server software found can only be seen as indicative.

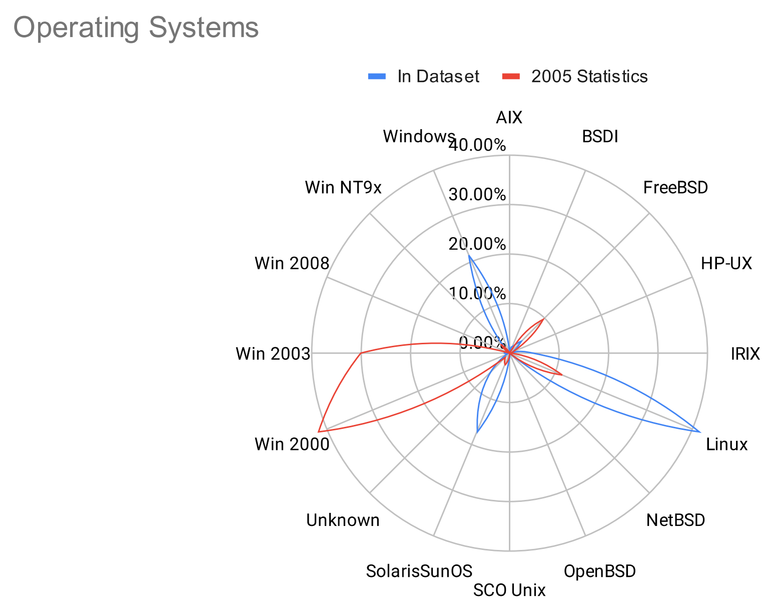


Figure 4.8: Comparison of Operating Systems mentioned in the research dataset (blue) and the 2005 overall statistics (red)

As an approach which factors in both the uncertainty of data and the lack of usage data for both operating system and server software for each year, the metadata from the dataset will be compared to the general statistics of attacked operating system and server software released by Zone-H in the form of an annual report since 2005 (Almeida 2008).

The result shows a discrepancy between the Windows operating systems (Windows, Win NT9x, Win 2008, Win 2003, Win 2000) and the Linux operating systems. While in the research dataset, over 40% of all defaced pages reported back to the crawler to be running Linux, this figure is only slightly above 10% in the general statistics. It is possible that some distortion is due to the focus of the

[32] For more information on this standard procedure of hardening (securing) a Web server, see Sciberras (2019).

research data set being around the years 2000-2001, before the release of Windows 2000 and 2008. Still, this Windows versus Linux profile is contrary to what Zone-H reports:

> In the past the most attacked operating system was Windows, but many servers were migrated from Windows to Linux…Therefore the attacks migrated as well, as Linux is now the most attacked operating system with 1,485,280 defacements against 815,119 in Windows systems (numbers calculated since 2000). (Almeida 2008)

The reasons behind this phenomenon are unclear. One suggestion would be that defacers active in political campaigns choose their targets differently than defacers interested in hitting as many pages as possible. Underlying this is the assumption that Linux-based operating systems are commonly understood as state of the industry web hosting platforms, with Windows web hosting enjoying a more casual, less secure reputation. More data is needed to substantiate this assumption though.

Another piece of information extracted during the crawl and added to the metadata is the server software found on the target. Knowing what software and version is running on a target would be very important for any attacker as that allows for the exploitation of known vulnerabilities. Similar to the operating system, it is thus considered good practice to not reveal the server software and its version to visitors. Also similar to the case of the operating system list above is the general lack of data availability as it seems pages originating in older collections such as alldas.de do not feature any information of the server software. In the research dataset, over 90% of all pages do not feature metadata information on the server software, while only 0.28% of the entire Zone-H archive in 2005 lacked this metadata. The following figure shows the two profiles, comparing the research dataset to the 2005 statistics:

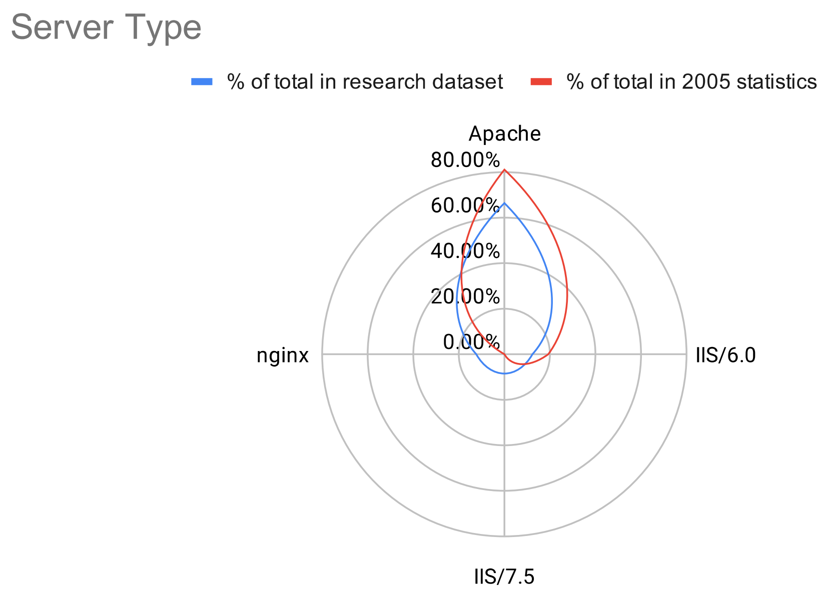


Figure 4.9: Server type as recorded during the crawl, where data was available

As can be seen, there is nevertheless little discrepancy between the research dataset and the 2005 statistics. Generally, the Apache Web Server is by far the most popular server software, reaching over 60% and 80% use respectively. It is noteworthy that despite the great variety in operating systems, almost all server software found is the open-source Apache, with Microsoft's Internet Information Services (IIS) only having a marginal share. This seems to support Almeida's claim that by 2005 Linux had become the most important operating system for web hosting as Apache is primarily aimed at Linux operating systems.

Looking at the operating system and server type information in the metadata, different trends become apparent. While there exists a wide range of operating systems, there are only four different types of server software recorded. For operating systems, the 2005 statistics show a strong preference for Windows-based operating systems, while the research dataset shows an emphasis on Linux distributions. It was suggested this might be the result of a more deliberate target selection process, yet more data is needed to substantiate this. Regarding server software, there is little difference between the thesis dataset and the 2005 statistics. Generally, these metadata items are only occasionally available for early (pre-2005) defacements. Neither the operating system nor the server type metadata can be used as a single identifier of a political web defacement, however the hypothesis of a deliberate target selection in political web defacements was substantiated in the different operating systems profiles found in the sense that political web defacements target a different operating system/server software combination. The reason for this is assumed to be that political defacers are less likely to focus on less secure, more accessible Windows server but rather choose targets based on their symbolic importance even if that means spending more time on a single attack.

The analysis so far has produced an overview of the available metadata and contrasted that metadata to the submission statistics of 2005. This overview of metadata serves as the entry point for the coming content analysis and the case studies. It allows for every individually mentioned page to be positioned within the context of trends and campaigns in defacements. As part of this thesis' work is not only the individual analysis of defaced pages, but also the development of a research methodology for ephemeral and non-traditional web content, the next section will now move on from the discussion of metadata to a discussion of content analysis to survey the research data set.

4.3.8 Automated content analysis

Natural language constructs most of its higher-level meaning through differential signifiers (cf Saussure, Bally, and Baskin 1966, 65–70).[33] In NLP, the closest approximation to a signifier is a token, described as "an instance of a sequence of characters in some particular document that are grouped together as a useful semantic unit for processing" (Manning, Raghavan, and Schütze 2008, 23). In the upcoming section, only individual tokens have been processed and their difference has merely been assessed in terms of frequency. The analysis has thus acted in the sense of what Barry describes as the softwareization of society (2014, 72) as it has transformed a natural language assembly into a series of machine-processable tokens. This must be considered before there can be any talk of meaning or results. It is important for any research to clearly understand the capabilities and limitations of its methods. In the case of natural language processing, the difference between the system output and the user interpretation must be appreciated. Analysis de-contextualises words by abstracting them into tokens whereas meaning comes from context. There are results, sure, and these results are the consequence of the applied methods. If the methods were chosen appropriately, the results can be useful depending on the object and objective of the study. To talk about meaning in the context of natural language processing word counts though implies that one has become softwarized themself and sees in natural language nothing more than what a computational system can see. For such a school of thought, the answer to a lack of meaning in an automated analysis is the increased use of computational methods, since

> within a computational society, the answer to a crisis of computation is turn to intensified computationality, that is greater use of softwarization… (Berry 2014, 82)

In other words, it is the belief that, given enough computational resources, all of Saussure's differential signifiers can be mapped out to arrive at an understanding of language. Meaning is thus a word to be used carefully in that context. In the following section, it is not the aim to portray any combination of numbers as the essence of the corpus. Rather, any data or findings must be seen as consequences of the applied methods, blind and oblivious to anything which could not be softwareized.

[33] Also see Eco (1984) and Merrell (2016).

4.3.9 Token frequency

To gain a first overview of the content of defaced pages beyond the results of the metadata analysis, the occurrence of words throughout the entire research dataset is recorded and put into relation. This process of language modelling is known as n-grams (W3C 2001) and is used as a standard practice in natural language processing. (Bird, Klein, and Loper 2009; Perkins 2010) The term natural language in this case relates to text written for and by human actors and excludes text written for machines such as the HTML tags which make up a web page. While it is possible to reverse the approach and construct a corpus of HTML tags, because of the relatively simple technical structure of most defacements it was decided to focus on the natural language rather than artificial language in the dataset. For the purpose of this study, the process has been structured as follows:

- The HTML source of a defaced page has been stripped of all HTML tags. All punctuation has been removed and all remaining text is converted to lower case.
- The text has then been divided into individual tokens by the processing library. Ideally, all tokens are unique English words.
- A custom list is used to filter out non-meaning-bearing tokens such as auxiliary verbs, articles and leftover HTML elements.
- Now all remaining tokens are written to a list and from there on can be aggregated and counted.

A graphical representation of the token frequency for the research dataset is shown below:

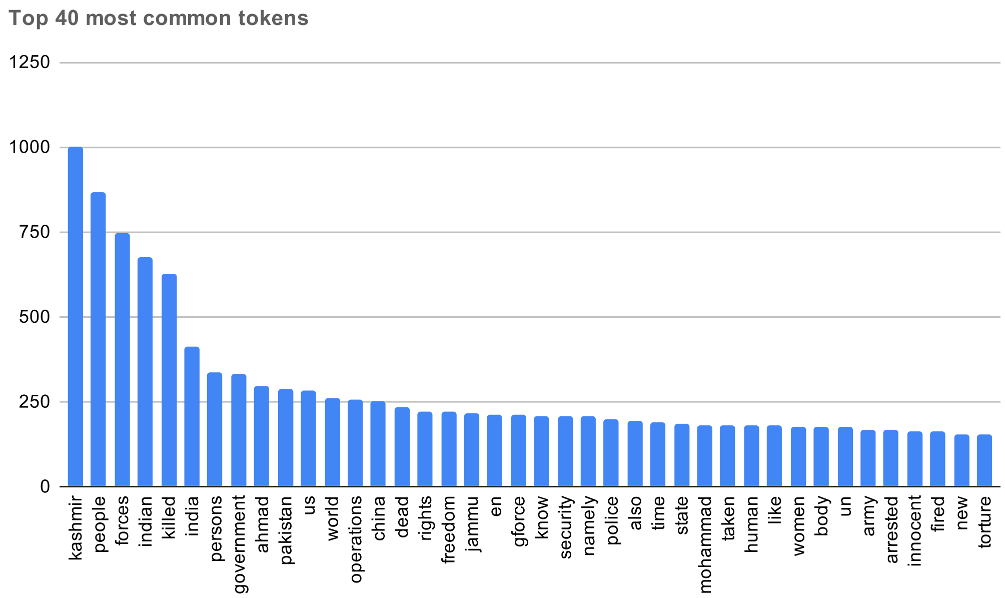


Figure 4.10: The 40 most common tokens in the research dataset after processing and filtering

The figure shows five distinct tokens (kashmir, people, forces, indian/india and killed) with high occurrence, and a plateau of the other 35 tokens. These results can be further broken down into places (kashmir, india, pakistan, world, china) institutions (government, police, state, un, army) and verbs (killed, taken, arrested). Even at this high level, the n-gram analysis gives a first overview of the content of a large set of defaced pages – defacements around the Kashmir conflict are indeed the most numerous, while the most active defacement group GForce is also featured in the top 40 token list. The high concentration of especially the first five tokens can also be seen as a sign of the coordination of campaigns, where groups use templates to quickly fill defaced pages with content. The use of templates to increase defacement output in coordinated groups is confirmed by Maggi et al. who state that:

> our key observation is that deface pages within the same campaign are very similar to each other, if not identical. This is a strong attribution indicator, which allows the analyst to group them together and understand the relationships between teams and actors. [...] From hereinafter, we use the term campaign template (or, simply, template) to indicate the content (e.g., bits of text, color scheme, language, character encoding) that is common to most of the pages within a campaign, which in turn can be leveraged to recognize and identify each campaign. (2018, 446)

The observation by Maggi et al. can only partially be confirmed through analysis of the research dataset. While it is true that defacements submitted by GForce in the context of the Kashmir conflict feature high degrees of similarity and seem to have been created drawing on multiple pre-made snippets of text, it cannot be confirmed that the use of templates is a common practice across defacer groups. Other influential groups such as BHS and AIC re-use certain elements such as logos and slogans, but on a scale too small to be featured in the n-gram list. The problem of attributing pages to defacers mentioned by Maggi et al. is easily solved by the fact that defacers are looking for recognition through their work so that even in the absence of identifiable metadata authorship is explicitly claimed and does not need to be constructed through text similarity.

As insightful as the list of tokens is for identifying the importance of pages around the Kashmir cluster, no strong indication on any 9/11 themed defacements are found. Only in hindsight can unspecific tokens such as army, un, world, innocent, etc. be interpreted as maybe belonging to the 9/11 cluster. It is further doubtful whether such an unspecific approach can be used successfully on a much larger dataset where multiple campaigns of similar size make it more difficult to identify one single topic. Generally, textual heterogeneity, non-standard spelling and a diverse range of topics and opinions make it hard to extract individual groups or campaigns. What the n-gram view provides for the assessment of the research dataset is a first overview of the most referred to topics, institutions and actions. Contextualizing this data further means to put any token occurrence into relation to the overall token count, to arrive at token frequency. In the next two sections, the frequency of tokens will thus be contextualized to show tokens over time as well as tokens occurring in combination.

4.3.10 Token combinations

Two tokens appearing together are described as bigrams in natural language processing (Perkins 2010). Bigrams are counted after all stopwords and punctuation has been removed, so that a sentence like “The cat on the table” turns into “cat, table” in the same way that “The cats had been on a table” is also turned into “cat, table” since plurals are turned into singular and auxiliary verb constructions are removed. Because of these processes, bigrams are not snippets of the original corpus, but are token combinations. The use of bigrams allows a more fine-grained look at the corpus while making a first step from a mere count (as the n-grams or mono-grams of the previous section did) towards a pattern analysis. A visualization of bigrams for the research dataset shows the following distribution:

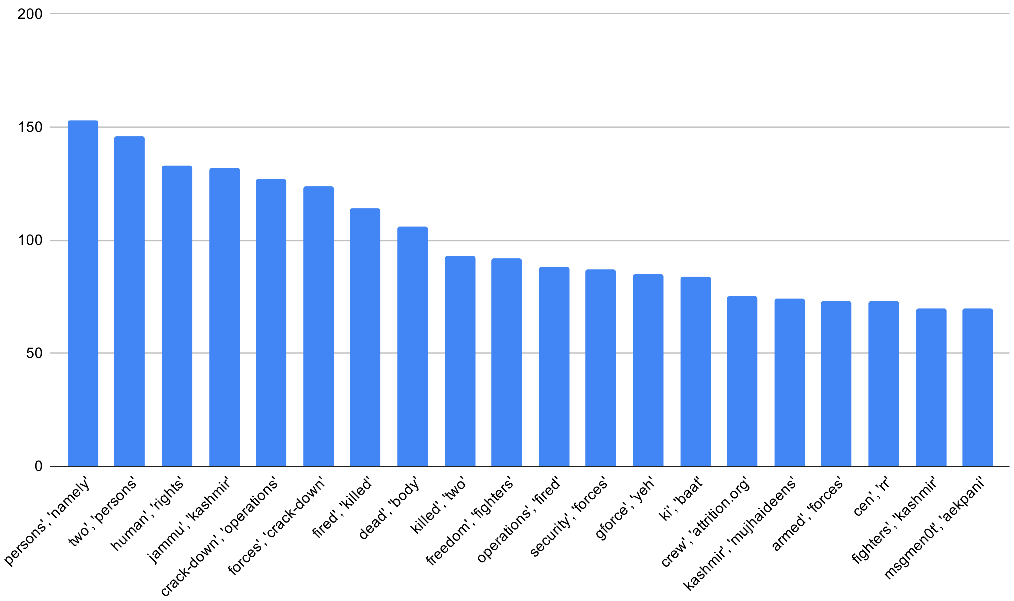


Figure 4.11: Top 20 token combinations (bigrams) for the research dataset after processing and filtering

Token combinations naturally occur less often than individual tokens. This is expected and the number would further decrease if three- and four-token-combinations were analysed. While the top token in the individual list is "kashmir", here it only appears in fourth place with the combination "jammu, kashmir"[34]. The token appears again in the more expressive combination "kashmir, mujhaideens" and "fighters, kashmir". This shows how the bigram list can complement the token frequency and help contextualize tokens. The bigram list also paints a much darker picture of the content of the research dataset, featuring common token combinations such as "crack-down, operations", "fired, killed", "dead, body", "armed, forces" etc. Its top combinations show interesting detail that was lost to the individual token frequency: the two most common combination ("persons, namely" and "two, persons") indicate that these defacements talk more about individuals and individual fate than about larger, more abstract groups such as states, regions or movements. This indication aligns with the theoretical framework of the analysis of web defacements as antagonistic writing in a struggle over public memory, in which narratives about individuals function both as prototypes of larger narrations as well as appeals to empathy and sentiment.

Similar to the token frequency, the bigram distribution shows a dominance of defacements centred around the Kashmir conflict in the research dataset. Like in the token frequency list, no direct references to any other topic are found. This for one confirms the significance of this topic for web defacements of the early 2000s, yet it also serves as a reminder that only defacements with high homogeneity will feature prominently in any frequency distribution.

[34] Describing the India-adminisitered territory Jammu and Kashmir (Akhtar and Kirk 2019).

It is telling that the combinations “gforce, yeh” and “crew, attrition.org” are featured in the bigram list and rank way ahead of combinations like “new, york” (rank 397) and “bin, laden” (rank 109). No other defacement group’s name is featured as prominently as GForce. This is testament to the group’s dedication in building a reputation and recognizable identity as well as their internal cohesion which led to a highly recognizable public profile. It is at the same time testament to the multi-layered function of web defacements. One motivation for defacers might be a genuine investment in the topic and viewpoint they are trying to promote. This can be seen in both the token frequency and the bigram list, where topical tokens such as Kashmir and human rights rank highly. Unaffected by this, a second layer of motivation might be the promotion of oneself and one’s own group as skilled and well-known hackers. The above data shows indication that both motivations played a role in how defacements were structured when self-promotion outranks more topical bigrams. As another example, there are 44 different bigrams featuring “owned” (in the context of “X owned your server”) in various configurations. This observation is important as it is one of the few moments in the study where quantitative arguments about defacer motivation can be deduced from the data.

4.3.11 Tokens over time

The distribution of tokens can further be broken down into token use over time. Doing so brings a new problem which the methodology must address. Since the distribution of defacements is very uneven and some years are not represented at all, tokens can no longer be compared by total count. Instead, token frequency is calculated by comparing a token count to the overall number of tokens available for each year. This approach allows us to compare years with high activity to those with low activity. This calculation of token distribution is a standard approach in natural language processing and is described by Bird et al. (2009) and Perkins (2010).

Following the calculation of token distribution, the most often used tokens per. year are compiled and their frequencies are added up. This gives a combined frequency which serves as an indicator of how widely used these tokens were for each year.

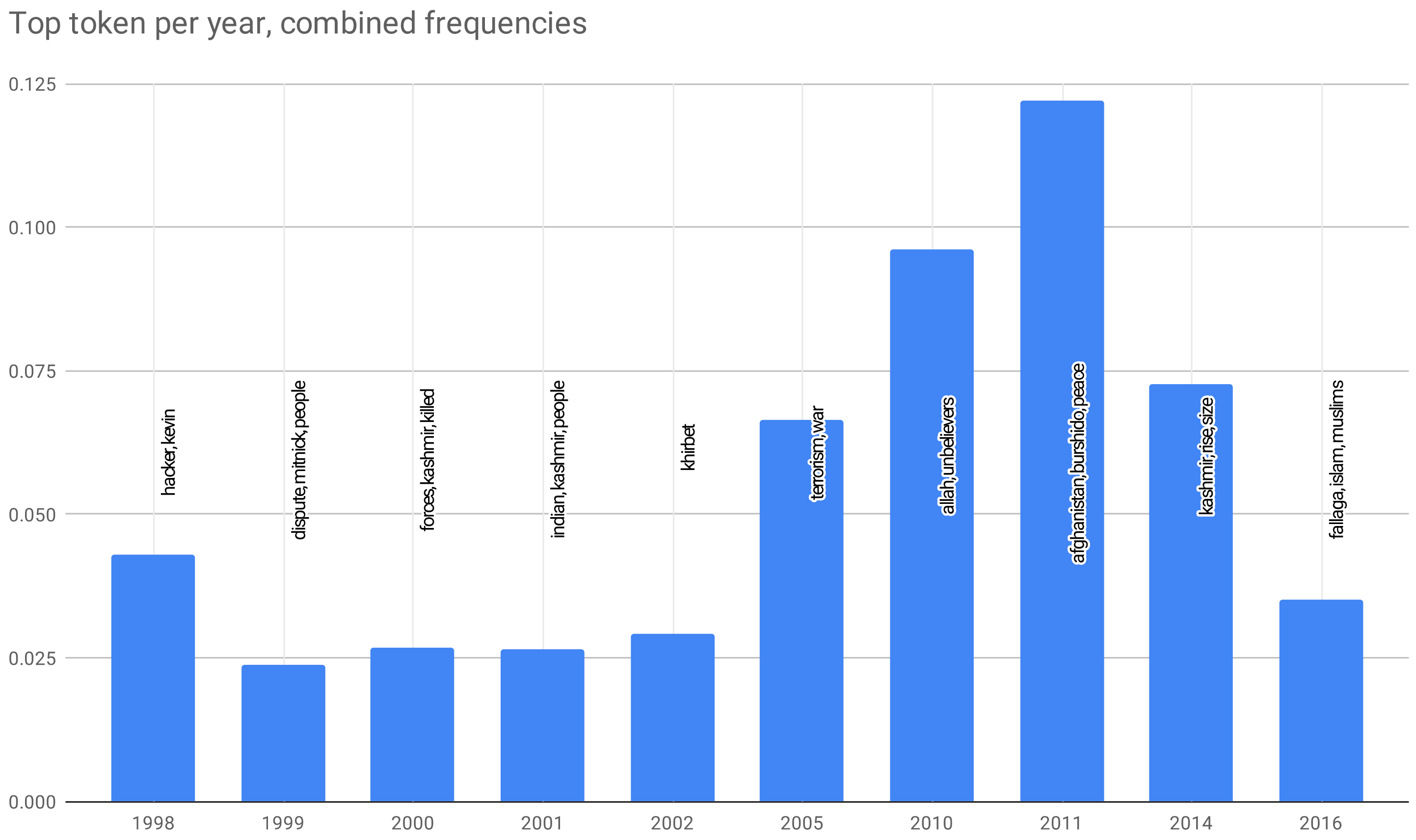


Figure 4.12: Top tokens per year, combined frequencies

The figure shows that some tokens are used throughout the years, while others appear only once. Tokens which feature more than once are: “kevin” “mitnick” (either part of his name), “kashmir” and “people”. The data shows how important the trail of news coverage around the arrest and imprisonment of hacker Kevin Mitnick was for pre-2000 defacements, while the Kashmir conflict appears as a token in 2000, 2001 and 2014. Past 2005, religious conflict (seen in the tokens “allah”, “unbelievers”) can be seen, while “afghanistan”, “burshido” (a defacer) and “peace” rank highest in 2014. This shows a turn away from scene-internal communication towards geopolitical events and also suggests a change in the audience defacements were aiming to reach by featuring geopolitical events over scene-internal events.

The combined token distribution frequency is an indicator of how thematically focussed defacements are for each year. It is striking to observe the rise in that specificity between 2005 and 2014 where over 10% of all tokens were either “afghanistan”, “burshido” or “peace”. Token frequency is thus a good indicator of how thematically diverse defacements are and how many other topics were mentioned each year past the top three tokens.

The tokens in general give an indication of the topics addressed in defacements for each year, but they also show topics beyond what in the broadest sense can be described as political expression. The tokens “hacker” and “burshido” suggest that self-referential topics play a role in defacements as well. The question is whether self-promotion and internal communication are antagonistic elements to political expression in defacements or whether they are part of defacer habitus.

While motivations may work on different levels, and the motivation to show off may not exclude the motivation to express one’s political viewpoint, the above observation serves to support Samuel’s observation about defacer motivation: “hacktivists define their movement not by its goals, but by its methods” (Samuel 2014, 105). The question of defacer motivation will be dealt with in more detail in the following section.

4.3.12 Metadata: Conclusion

The aim of this metadata analysis was to survey the usefulness of existing and newly created metadata in identifying foci for further research. To this end, the existing data as provided by Zone-H was aggregated and visualized. Where appropriate, the result was contrasted with the overall statistics released by Zone-H for the time period from 2005 to 2007. The metadata provided with the defacements is exclusively focussed on the attacker and circumstances of the attack. As such, it is useful to identify peaks in activity, the appearance and disappearance of defacer groups and a target profile as expressed through the TLD distribution.

Implied in this analysis was the question of scalability, whether such an analysis could be replicated on a larger dataset with the intention to identify relevant defacements. This pilot study has demonstrated the capabilities of this methodology to identify relevant groups, time periods and topics in a data set of any size. With all its limitations, which have been described above, the available metadata retains the advantage of being easily attributable to individual defacements and thus holds the potential to be key in identifying relevant defacements in a hypothetical, much larger dataset.

Beyond the metadata bundled with the defacements, part of this section was dedicated to creating its own metadata in the form of tokens. These tokens derived from the text of defaced pages, were processed according to NLP standards and aggregated by count and frequency. It was shown that this approach is useful for identifying topics, while token combinations gave a first understanding of attitudes and contexts used in defacements. Finally, the combination of relative token frequency over time provided insight into not only the most commonly used tokens, but also gave the relative specificity, which is indicative of the thematic diversity for each year. The token analysis proved to be a valuable counterpart to the exclusively attacker-focussed metadata obtained from Zone-H. In relation to scalability, token analysis is well suited for a computational analysis of the entire corpus and allows the researcher to identify thematic clusters.

A part of metadata which is collected by Zone-H, yet not attributable to individual defacements, is the reason or motivation behind an attack. While some of the previous section was hinting at reconstructing defacer motivation, the available data allowed for little more than speculation. As the token frequencies have shown, self-promotion and internal communication seem to overlap with political expression. To arrive at a more nuanced understanding of defacer motivation, the following section is going to develop and deploy a framework for the analysis of defacer motivation.

4.4 Motivation(s)

Reasons for defacing pages are diverse and work on different levels, not all accessible to the researcher and obscured by temporal distance and questionable metadata. A defacer hacking an Indian website may, for example, very well do that for political reasons but unless explicitly stated on the defaced page, that motivation would hardly be found out. The following section will investigate defacer motivation where possible, using extracted metadata as well as my own analysis.

4.4.1 Available metadata

This section about defacer motivation diverges from the approach used so far in the metadata analysis, which is to collect available (meta)data from Zone-H and compile it into statistics to generate understanding. The only data available on motivation provided by the source is a compilation of defacement reasons that notifiers can choose from – in itself an organizing and reductive principle:

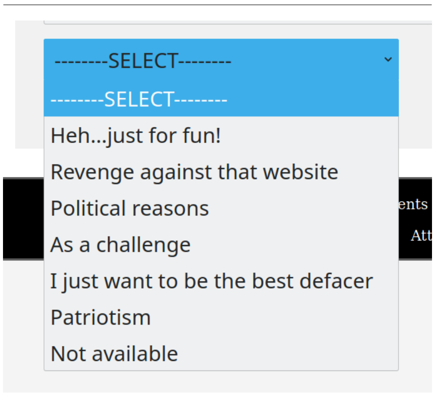


Figure 4.13: "Reasons for Defacement".

A notifier has to choose one of these when submitting a page.

Whatever choice is made does not become part of the metadata, but aggregated and released in yearly statistics. These statistics will be discussed in the following section. There is no option to either select more than one answer or add free text. It is unknown if and when these answers have been changed or expanded. It is obvious that these options yield little value for the understanding of political web defacements for their lack of specificity and, most importantly, their isolation from the rest of the data and metadata. For a quick classification, the answers “Heh...just for fun!”, “As a challenge” and “I just want to be the best defacer” point towards non-political activity aimed at personal achievement or building a reputation. The answers “Political reasons” and “Patriotism” hint at defacements in scope for this study, while the remaining two – “Revenge against that website” and “Not available” – are unspecific. It is unknown why patriotism received its own option outside the “Political reasons” option, although it hints at Zone-H’s assessment that patriotic defacements are somehow not political.

Visualizing the yearly release for the years 2005 to 2007 – the years closest to the timespan covered by the research dataset – gives the following figure:

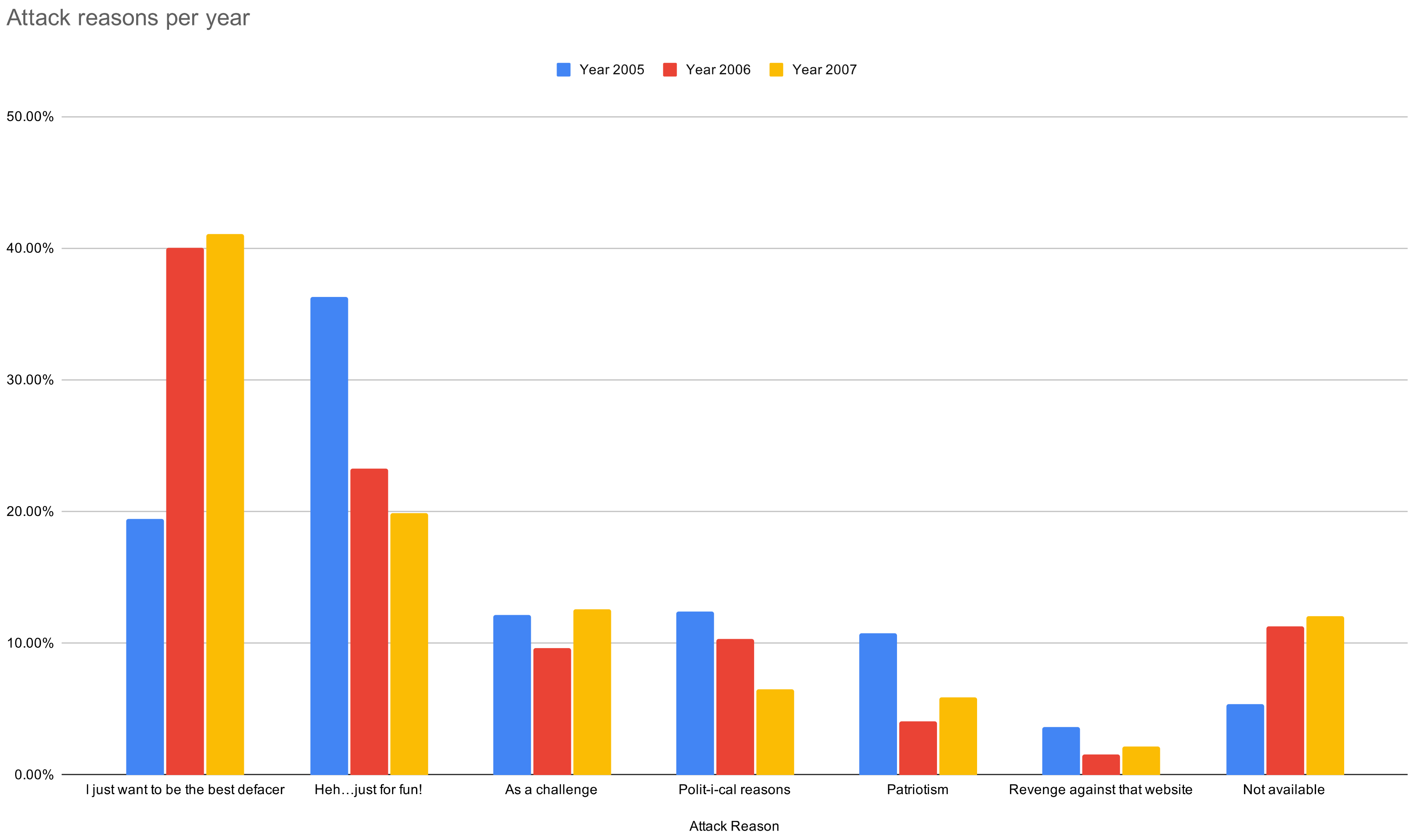


Figure 4.14: Attack reasons per year as per Zone-H's statistics report (Almeida 2008)

Focussing mainly on the answer options which may lead to political content as per the scope of this research, the two options “Political reasons” and “Patriotism” both decline from 2005 on and are, for every year, clearly outranked by the two main reasons.\ (“Want to be the best” and “Just for fun”). Still, these figures combined suggest around 10 to 20 percent potential political content for each year, a far cry from the research dataset which yielded around 0.02% relevant content. The suspected reason for this discrepancy is the different definition of a political or patriotic defacement. Since the field is mandatory, and the “just for fun” option is the first in the list, it might also be that notifiers choose it to get past the form as quickly as possible. The discrepancy also suggests that the attack reasons as given by the notifiers are not necessarily reflective of the defaced page’s content. If anything, they can describe trends such as that political reasons for defacements are becoming less important as a whole while competitiveness overtakes hedonism as the number one attack reason. Generally, defacement numbers rose from about 494,000 in 2005 to 752,000 in 2006, before dropping back down to 481,000 in 2007 (Almeida 2008) without this 2006 spike leading to a clear rise in any of the reasons. This links back to earlier observations of scene-internal communication being as important as scene-external communication.

4.4.2 A custom approach to the question of defacer motivation

It has become clear from a brief look at the available metadata on motivation provided by Zone-H that no satisfactory answer to the question of defacer motivation can be deduced.[35] This implies that a custom approach is necessary to understand motivations. The approach described in the following works exactly in reverse order to the one described above: instead of the defacer providing a statement of motivation together with the URL of a defaced page, this approach starts with the archived page and attempts to find clues regarding the author’s motivation. It does so by using a combination of criteria which are combined to form a matrix describing the characteristics of a page in more detail and with more granularity than the mono-causal approach described in the above section. This allows the capture of multi-layered motivation as much as changes in motivation over time and avoids generalisations about web defacers.

[35] With all the critique on Zone-H's metadata recording, it needs to be stated that the site is not and never was intended to be a Web archive in the academic sense. It is the largest and the most active defacement archive on the Internet and critique of the available data does not undermine the efforts that went into building and maintaining the site for over 15 years.

Motivation is, as has been said, multi-layered. Drawing on work by Alexis Samuel regarding web defacer identity and motivation, the following incentives are at the core of this custom approach:

Incentives	**Description**	**Application**
Ends-oriented incentives	Participants' desire to accomplish the anticipated collective or public outcomes of collective action.	Pages are tagged according to their communicative function.
Expressive incentives	The psychological and/or emotional benefit of expressing one's political or social values through political action that reflects those values.	Pages are tagged according to the field or topic the expression is aimed at.
Interactive incentives	The enjoyment of participating in an activity that involves interacting with other people.	Pages are tagged according to the existence of greetings/shoutouts and messages to other hackers.
Solidary incentives	The psychological and/or emotional benefit of belonging to a group that shares one's political or social values, or of fulfilling the expectations of one's social network	Pages are tagged according to the existence of a message aimed directly at the enemy or the statement that no harm was done to the original site.

Table 4.2: Incentives in web defacements, based on Samuel (2014, 118).

Samuel also describes material (here: financial) incentives, which may play a role in defacements either in finding employment through one's renown or in the case of a sponsored defacement group, but no case of material incentive has been found in the research data set and thus this incentive has not been developed further.

The above incentives are then translated into criteria relevant to the research dataset. During this process, some incentives are mapped onto multiple-choice options while others are binary options. The process of mapping is explained in the following:

Ends-oriented incentives	**Description**
Spread information	The page is primarily concerned with providing information (whether true or false); no or very little judgement is made.
Expression of anger	The page is a reaction to an event; it's primary function is to express anger.
Accusation	The page is directed at a perceived enemy, accusing them.
Argument	The page provides information in order to make an argument; goes beyond the mere provisioning of information as seen in the Spread information type.
Memorial	The page is dedicated to the memorial of tragic events or individuals.
Call for help	The page urges institutions (usually UN/US) to intervene in a situation.
Support	No clear focus, expresses support for a cause.
Call to action	The page urges the viewer to take action.
Raise awareness	The page aims to raise awareness of what the author sees as a forgotten or under-reported event.
Undefined	Page where no clear focus could be determined.

Table 4.3: Mapping of ends-oriented incentives onto the research dataset

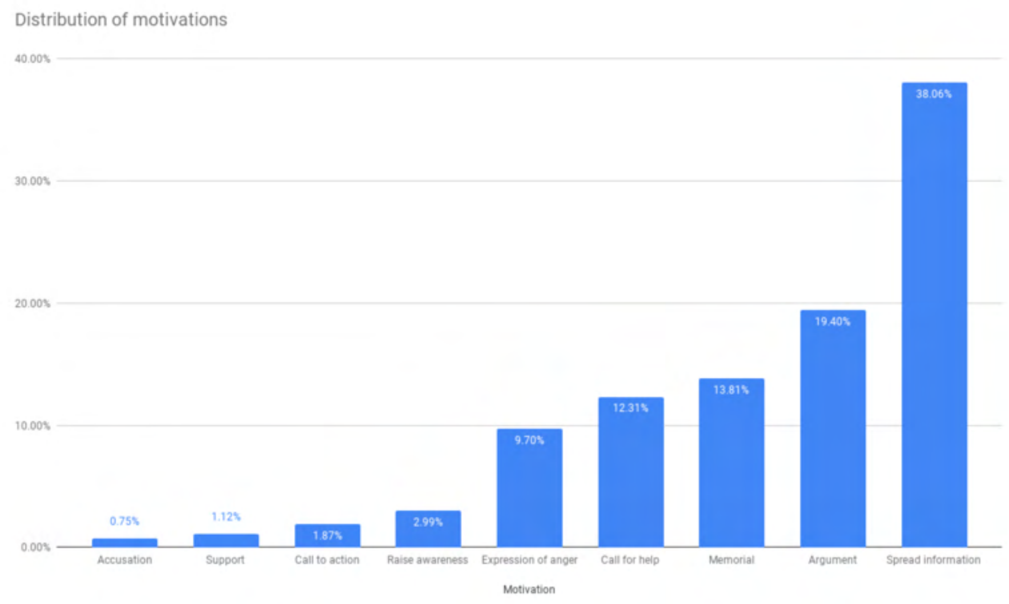


Figure 4.15: Types of ends-oriented incentives as percentage of total

The above figure visualizes the occurrence of the described types of ends-oriented incentives as percentage of the total. It shows that 38.06% of all defacements in the research data set are primarily concerned with the spreading of information, that is the provision of information without immediate judgement. The second most common type is similar to the first, but uses information provided to form arguments and thus includes a distinct judgement based on the provided information. Two more types – the call for help and the memorial – are closely related to the more general spread information type, yet they are distinct in that they are a specific message sent out to the viewer to either take action by contacting authorities or to remember a person or event.

The call for help type is important to understand the perspective and framework from which defacers operate. The type is, as described above, defined by a message to states (mostly US) or institutions such as the EU or UN to take action in a particular conflict with the hope of ending violence. Often this type is accompanied by elements taken from the argumentative type or the memorial type. It is an expression of their value system when defacers, often hacking from the global South, attempt to bring their issues to the attention of these Western institutions in the hope that availability of information will lead to improvement of real-world conditions. On a technical level, this shows thought rooted in ideas of information capitalism and the softwareization of the material (cf Berry 2014), yet on a political level shows a great degree of Habermasian thought about the function of information availability as the precondition of a political public sphere. This aspect is worth dwelling on, because it showcases a lineage of thought from counterculture to hacker culture:

> In the late 1960s and early 1970s, intentional communities tended to be organized along one of two lines: either free-flowing anarchy or rigid, usually religious, social order. Both types of communities, however, embraced the notion that small-scale

> technologies could transform the individual consciousness and, with it, the nature of community. (Turner 2006, 74)

Ideas of free-flowing energies as the driving force of a community were prevalent in the scene from which an amateur computing and hacking scene would soon develop. This idea of self-regulation through technology must be seen against the backdrop of an increasingly deregulated market and reinforced by the first software companies based on these principles. Note that Turner speaks broadly of free-flowing social order and small-scale technologies. These concepts become more concrete over time and eventually morph into an understanding of the Internet as a technology both small-scale in the sense that it was relatively cheap and easily accessible and transformative in the sense that it embodies the free-trade ideal of deregulated exchange:

> Thomas Frank has termed this vision "market populism," and as he has indicated, in the 1990s it depended on a particular reading of the Internet. If the market was to be a deregulated mechanism of political as well as economic exchange, the recently privatized circuits of the Internet, with their free-flowing streams of commercial and noncommercial bits, made a perfect rhetorical prototype of the market-populist ideal. By the end of the decade, the libertarian, utopian, populist depiction of the Internet could be heard echoing in the halls of Congress, the board rooms of Fortune 500 corporations, the chat rooms of cyberspace, and the kitchens and living rooms of individual American investors. (Turner 2006, 215)

Returning to the call for help and spread information type defacements, it becomes clear why defacers rely on it as much as they do, their scene being built on both described predecessors, counter and hacker culture. What Berry describes as a softwareization of society, where each crisis is believed to be resolvable by applying more or more refined methods of computation, is actually the lineage of the techno-utopian belief in the transformative power of technology mentioned by Turner.

With the above in mind, both types (call for help and expression of anger type) cannot simply be dismissed as lack of life experience or class consciousness. Taking these two types together with the less specific spread information type, it is evident that the vast majority of defacement are expressive in the sense that their primary function is to send information outwards. On a political level, this is not done in the form of manifestos or demands, but rather is done in the form of information provision aimed at a public sphere that is assumed to share universal concepts such as human rights and national self-determination.

This finding lies at the core of defacer' motivation at large. Their goal is to start or influence a public debate about a particular subject based on the assumption that a public sphere sharing the same universal beliefs will eventually arrive at a conclusion favourable to the defacer's interest if only enough information is made available. This leads back to the libertarian nature of hacker culture, where free-flowing information is seen as the prerequisite of effective government. This finding becomes very important when considering the temporal distribution of such ends-oriented incentives:

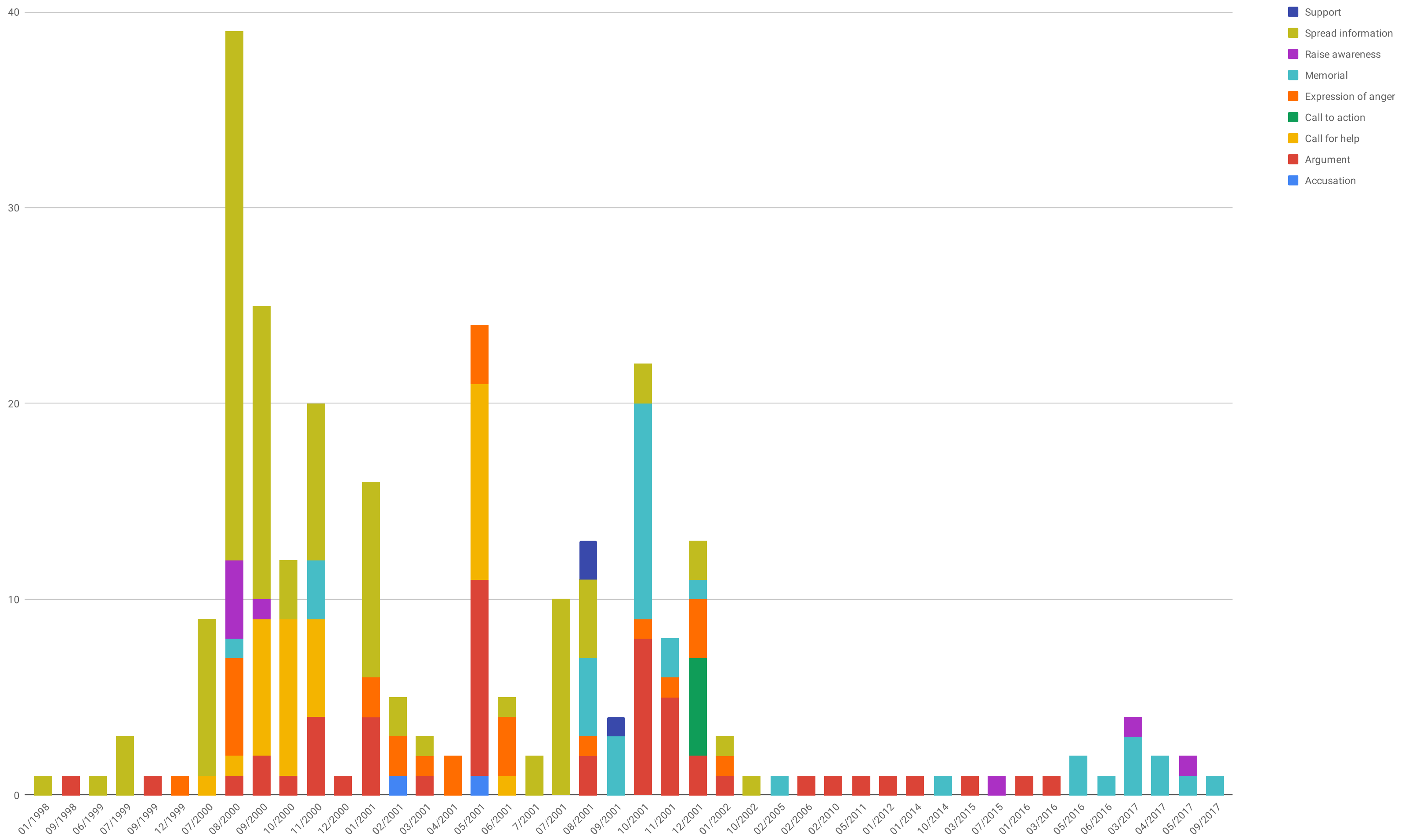


Figure 4.16: Ends-oriented incentives over time, excludes undefined

The figure shows a distinct peak in the spread information type in August 2000. Most of the defacements submitted at that time were related to the Kashmir conflict while the second smaller peak in late 2001 is 9/11-related defacements. The information type peaks in 2000 and then begins to decline, until it is no longer found from October 2002 on. Almost at the same time, the call for help type peaks (August 2000 to October 2000) to then disappear again after June 2001. A type gaining popularity in the early 2000s is the memorial page which peaks in the 9/11-context and re-appears later in 2016 to 2017 in the context of the Syrian civil war.

This figure is not the result of one individual defacer abandoning ideas of public sphere participation but is the result of a general shift in web defacement regardless of their topic. In terms of incentives motivating defacers, there seems to have been a move away from simple provision of information towards the more specialized memorial of individuals. The more audience-focussed call for help follows the same trajectory and seems to have been eventually abandoned.

What can be deduced from this data is that defacer motivation is diverse and changing over time. Fluctuation, peaks and changes in motivation can be observed. This confirm findings of the literature review that the common, uniform portrayal of hackers is incomplete. While there seems to be a constant stream of argumentative types, the motivation to spread information in various form seems to have lost much of its appeal. Its place is filled by the more narrative-driven memorial type of defacement. These findings also help explain why there is a general decline in the number of web defacements. As affective types of incentives replace more information-providing types, web defacements have lost part of their appeal since their characteristically unpredictable audience and short life span make them less suited for the development of a coherent narrative.

It is possible that this is a reaction to a more widespread use of the Internet and the general availability of information (cf Castells 2010; Andrejevic 2013). As information becomes ubiquitous, it is no longer an act of defiance to simply provide it without comment; in terms of influence it is the frame which forms information into Weltanschauung:

> the battle of images and frames, at the source of the battle for minds and souls, takes place in multimedia communication networks. These networks are programmed by the power relationships embedded within the networks… Therefore, the process of social change requires the reprogramming of the communication networks in terms of their cultural codes and in terms of the implicit social and political values and interests that they convey. It is not an easy task. (Castells 2013, 302)

What Castells describes here translates onto the dataset as the shift away from information-provisioning incentives towards more emotionally framed incentives – the memorial being the prime example here. The memorial incentive type does not aim to provide a full picture of any event, rather it sets the frame by carefully selecting aspects from the source material. Successfully launched, the frame generated by the memorial page will filter subsequent information and thus be more effective than the one-time provision of information.[36]

To deepen the understanding of defacer motivation, each ends-oriented incentive is further described by combination with an expressive incentive. In relation to the content of web defacements and the absence of concrete defacer statements, the expressive incentives are mapped onto the fields of the expression:

Expressive incentives	**Description**
Territorial	Expression in relation to conflict over a territory.
Political	Expression in relation to a political situation or conflict, more high-level than territorial
Human rights	Expression in relation to human rights violations.
Legislative	Expression in relation to laws and legal proceedings.

Table 4.4: Mapping of expressive incentives onto the research dataset

Expressive incentives occur across the dataset as shown in the following table:

Expressive incentives	**% of total**
Territorial	0.4%
Political	51.19%
Human rights	39.29%
Legislative	9.13%

Table 4.5: Expressive incentive occurrence as part of grand total

It is to no great surprise that with the scope of this study being political expression in web defacements, most expressions fit the broad political category. Where more specific expression could be detected, it is mostly regarding human rights (and the violation thereof). Smaller sets are concerned with legislative processes, either laws enacted (most referring to the *Patriot Act)* or laws applied such as in the case of sentenced hacker Kevin Mitnick. The smallest set are expressions directly aimed at territorial conflicts, mostly referring to Kashmir.

The expressive incentives in isolation, due to the scope of the research dataset, do not offer much additional insight. Their value lies in the option to create a matrix

[36] The concept of frames used throughout this study is based on the following definition:

> news frames, [are] representing persistent patterns of selection, emphasis, and exclusion that furnish a coherent interpretation and evaluation of events. […] Out of the myriad ways of describing events in the world, journalists rely upon familiar news frames and upon the interpretation of events offered by credible sources to convey dominant meanings, make sense of the facts, focus the headlines, and structure the story line. (Norris, Kern, and Just 2003, 4).

Also see Kelly (2012); D'Angelo and Kuypers (2010).

table that combines aspects from all incentives to find overarching patterns in the dataset. This approach is suited to overcome the problems of metadata dissociated from its source and only allowing for mono causal answers. Still, what can be observed from Table 4.5 are two clear foci beyond the broad framework of political expression. Additionally, expressive incentives specifically cover human rights and legislation in various forms. This is in line with the findings about the commonly-found appeal to authority in various forms found in defacements. Human rights and laws or legal proceedings are naturally well-suited topics for such appeals. It further shows a surprisingly high level of engagement with issues of human rights and the law, countering the image of individualistic cyber-hedonists hackers.

While all incentives appear in combination and could additionally be combined with the temporal distribution of attacks, this analysis will only do so where relevant results can be produced from such a combination. The combination of ends-oriented with expressive incentives is such a case where combination allows for a closer look at what fields of expression were chosen by defacers.

The first application of such a combination is the distribution of expressive incentives over time:

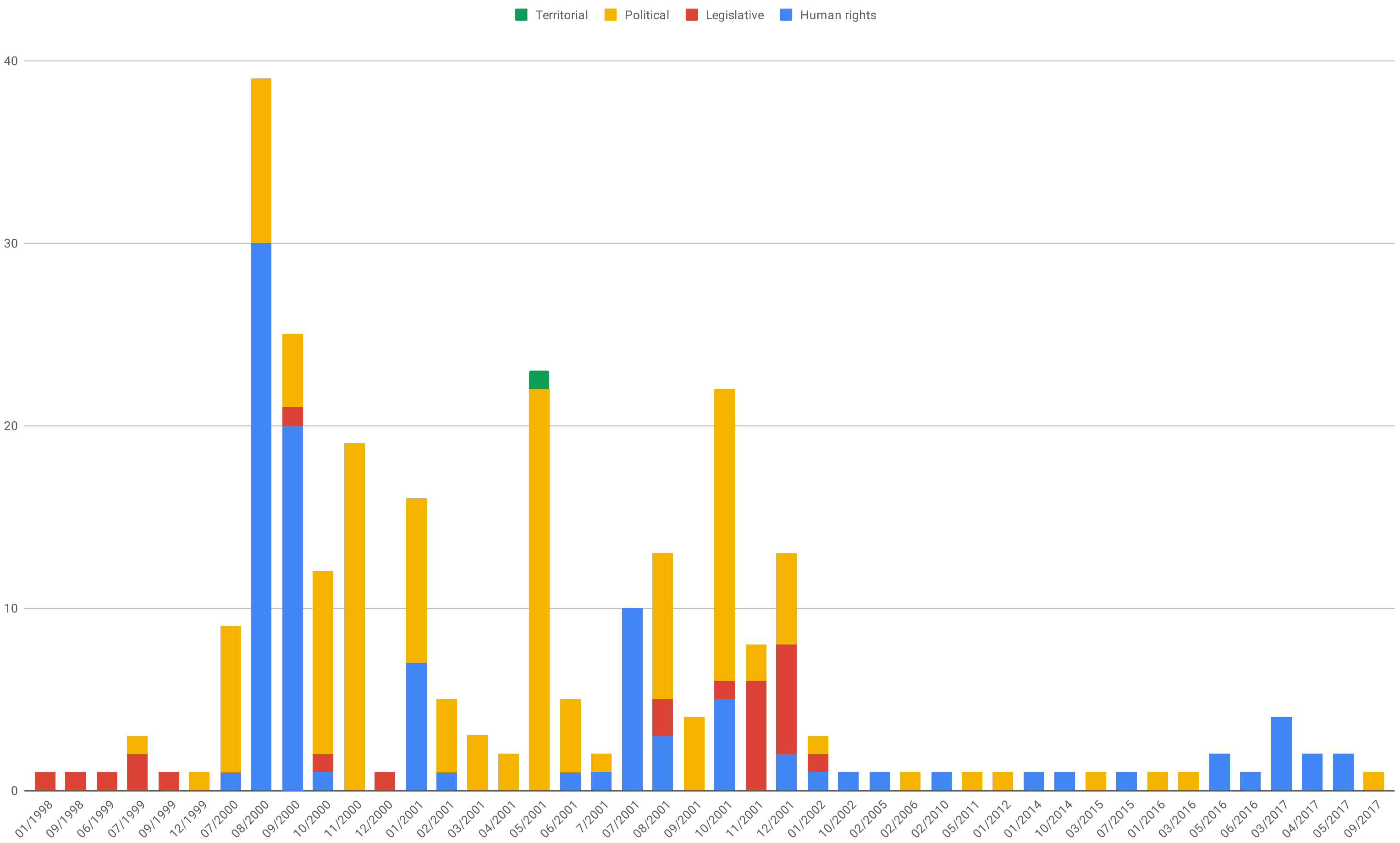


Figure 4.17: Expressive incentives over time

The figure shows that the field of human rights-related expressions makes up most of the first peak while the second peak of activity is much more heterogeneous. Expressions made in the field of legislation dominate the very early material in the research data set and re-appear in the context of 9/11 and the *Patriot Act* but are otherwise absent from the data. It is noteworthy that for the two peak periods of activity, expressive incentives usually appear in combination, while the small increase in activity from 2016 on is entirely composed of expressions in the field of human right awareness and violation. Looking at the visualization generally, it can be said that there is hardly a steady occurrence of any type, rather that types fluctuate and in some cases disappear for times. This makes defacer motivation in the field of expressive incentives more a reaction to an event than a phenomenon independent of real-world politics.

Combining the expressive incentives with the ends-oriented incentives allows for a closer look at the different types of motivation to be found in web defacements.

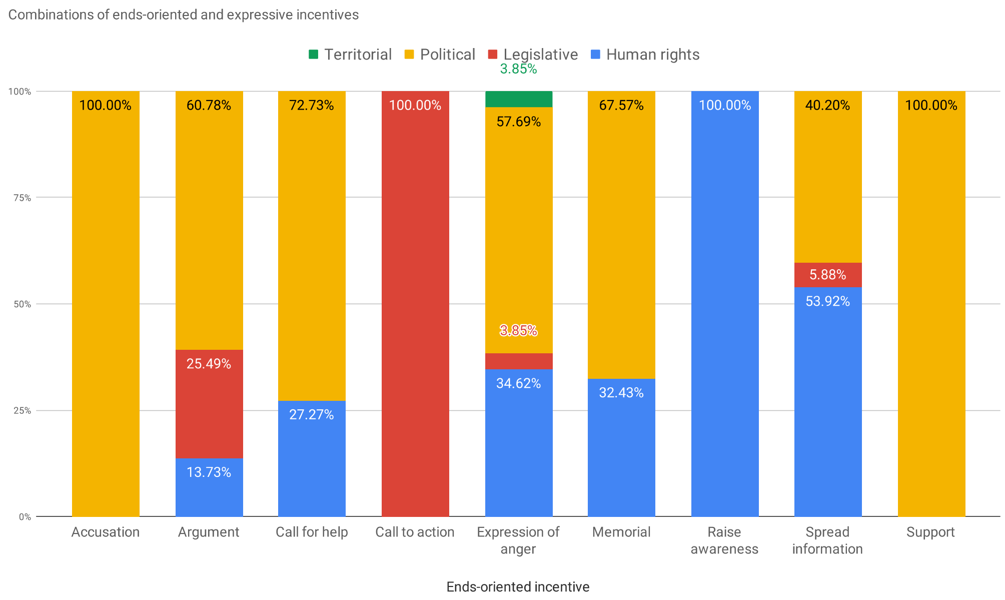


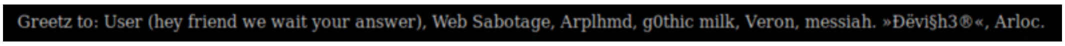
Figure 4.18: Combinations of ends-oriented and expressive incentives, stacked

The combination of ends-oriented and expressive incentives shows that while there are four types which exclusively fall into one field of expression, five ends-oriented incentives cover multiple fields of expression. Where that is the case (Argument, Call for help, Expression of Anger, Memorial and Spread information), it shows evidence of multiple different combinations of incentives that have led to the respective defacements. In the case of the argumentative type, the figure shows that three different combinations of incentives are present: political, legislative and human-rights related. Defacers might take up this specific type because they are driven by one or more of the three expressive incentives. No ends-oriented incentive features all four types of expressive incentive. The types that only feature one expressive incentive are Accusation (only political), Call to action (only legislative), Raise awareness (only human rights) and Support (only political). The singular expressive incentive in the Call to action type is reflective of the study's scope which explicitly defines hacktivism as less transgressive than (cyber)terrorism and thus excludes most calls to action that are not part of a democratic process, e.g. calls to take up arms. The Raise awareness type is a fitting type of hacktivist expression for concerns about human rights and confirms the observation from the ends-oriented incentive analysis that there exists a strain of defacements attempting to provide information with the implicit aim of influencing discourse through their presence. The types previously identified as narrative driven (Memorial, Argument) are more diverse in the types of expressive incentives covered and indicate that the described shift from information to affective provision extends through most of the range of hacktivist activity and is not limited to one group or one part of the political spectrum.

The combination of ends-oriented with expressive incentives gives a more detailed picture of defacer motivation. It shows that while some ends-oriented incentives cover only one field of expression, five out of nine cover multiple. The expressive fields of human rights and political events are covered by most of the ends-oriented incentive types, while the field of legislative proceedings is mostly covered by the argumentative and the call for action type.

4.4.3 Interactive incentives

Interactive incentives are mapped onto the research dataset by tagging the existence of messages directed at other hackers. This is usually done at the bottom of a page, in a section separate from the header (usually introducing the defacer) and the body containing the message. Interaction can also be negative, in the form of expressing disdain of other defacers. It is assumed that the presence of this greeting element shows a degree of interactivity between defacers, expressing both a knowledge of the scene at the time and a desire to communicate with the community. Going beyond the mere mentioning of other actors is the practice of leaving messages for other hackers on a defaced page. This ranges from threats to challenges to expressions of solidarity. All interactive incentives show a desire to interact with the community as much as the very special medium of a web defacement allows for.



Greetz to: User (hey friend we wait your answer), Web Sabotage, Arplhmd, g0thic milk, Veron, messiah. »Đëvi§h3®«, Arloc.

Figure 4.19: DefacementId 885, Greetings and message to others

Interactive incentives	**Description**
Greetings or like/hate lists	Features one or more greetings of other defacers
Hacker-to-hacker communication	Part or whole of the page directly addresses other actors within the scene, more specific than greetings.

Table 4.6: Mapping of interactive incentives onto the dataset.

4.4.4 Greetings

Combining the appearance of greetings with the submission dates gives the following figure:

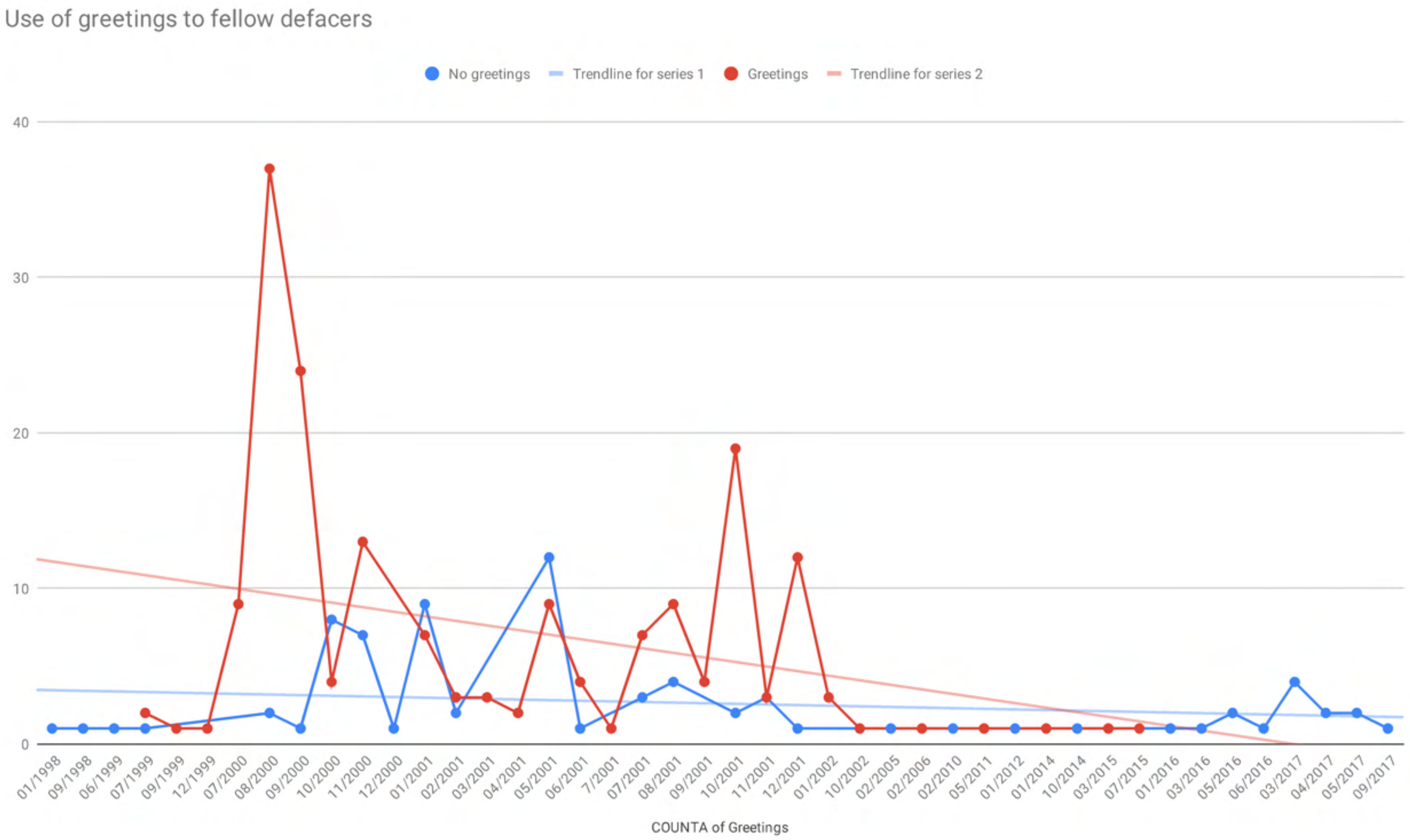


Figure 4.20: Presence/absence of greetings in defacements, trend lines added

The figure shows that the use of greetings, or expressions of sympathy and disdain, is common throughout the research dataset and occurs from July 1999 to July 2015. Usage of greetings has two distinct peaks between the end of 1999 and 2000 and again from September to November 2001. Very early defacements do not make use of the interactive element, nor do defacements after 2015. The use of greetings declines from the year 2000 on.

The data shows that the desire to interact with other defacers plays a part in motivating defacers during the key period of interest for this study. It can be assumed that this interactive element works in both ways; engaging with subcultural capital and appreciating other's work and seeking recognition for one's own work is rewarding for both sides. The fluctuation in the occurrence of the interactive greetings element also shows that different motivations existed within the scene over time, adding to the diversity of defacer motivation. Further, the fact that greetings are integral parts of many defacements, usually in the tripartite Intro – Body – Greetings structure, is evidence that motivations overlap and cannot be adequately described with a mono-causal approach. Just as greetings are not separate from political content, but organically appear together, defacers showing off their street credibility does not exclude defacers also wanting to send a political message. Defacer's motivation is multi-layered and may cover on one level the motivation to express anger over a new law criminalizing hackers while at the same time the desire to interact with fellow defacers and to maintain one's own reputation.

The widespread use of greetings requires a strong cohesion within the scene and a relatively stable system of aliases to function. It is easy to image that, if fellow defacers came and went too quickly, it would hardly be possible to send out greetings in this form. This is confirmed by Maggi et al. who find that "most of the defacers (80%) are devoted to the same affiliation(s) throughout their 'career'" (2018, 452) and by Samuel's expression of "robust pseudonymity" (2014, 230).

In conclusion, the use of greetings in web defacements shows that interactive incentives play an important role for defacers. This motivation overlaps with the other incentives described so far but seems independent from the actual field of expression or the content of the defacement. Using greetings suggests a high level of stability and cohesion within the scene. The fact that greetings become less popular over time suggests that this cohesion becomes less over time, while it also hints at the interactive incentive as a whole becoming less important for defacer motivation. While it cannot be deduced from the data which of the two is ultimately true – less cohesion or other channels of communication – it must be seen against the backdrop of the rise of social media from 2005 on and the increasing platformization of the web which offered new and easier channels to fulfil the need to determine social status within the community.

4.4.5 Hacker-to-hacker communication

More specific than greetings are defacements that partially or completely address other actors within the hacking scene. Usually this type of defacement is found in the context of legislative issues such as the trial of hacker Kevin Mitnick. Hacker-to-hacker communication in this form is distinct from the element of greetings as it uses most or all of the defacement to communicate within the scene, thus showing a very high degree of interactivity amongst peers.

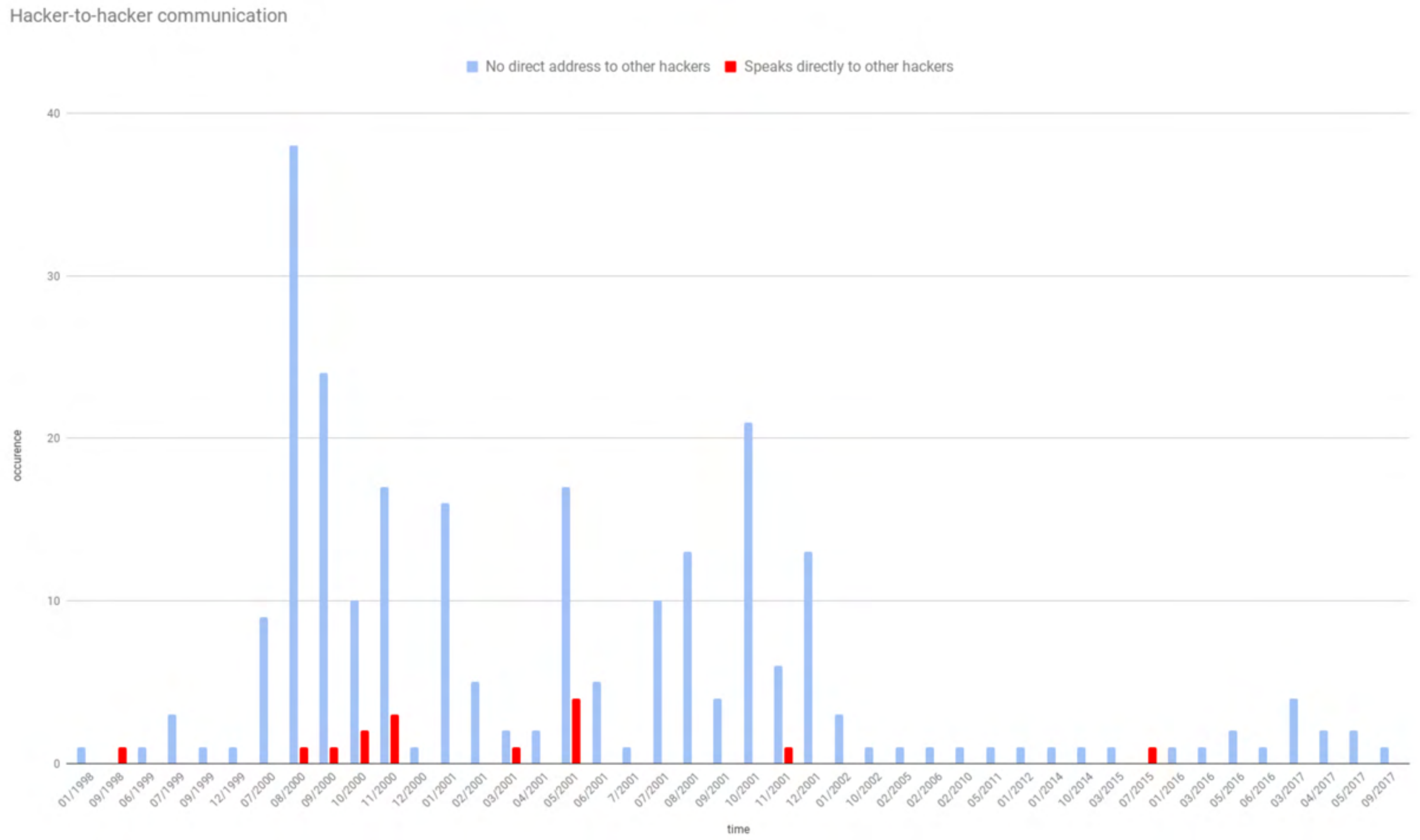


Figure 4.21: Part or whole of the defacement talks directly to other hackers

The data shows that creating defacements to communicate messages within the scene is rare, but nevertheless occurs at different times in the research data set. Instances where defacements speak directly to other hackers are generally not dependent on the overall defacement activity in that month and generally do not follow the rise and fall of greetings as described above. This leads to two conclusions.

Firstly, the above data implies that interactive incentives are important to defacers to the point where the author’s motivation for interactivity is not satisfied with mere greetings at the bottom of the page. This has led to a type of defacements that are meta-defacements in the sense that they are pieces of antagonistic writing of electronic text which address actors and processes in that field of antagonistic writing of electronic text. These defacements have as a distinct feature a surprisingly well-defined audience and a more efficient use of the web defacement as a means of communication, as the intended audience – other hackers – is likely to browse defacement archives such as Zone-H and will find these pages long after the original pages have been restored.

Secondly, hacker-to-hacker communication in web defacements is evidence of a self-aware scene that follows internal developments and observes itself. The data can, in that sense, add a piece to the question of whether defacements are formalized expressions talking to like-minded hackers or whether they are intended as nonconformist interjections in a public discourse. Looking at the existence of these meta-defacements, both strains can be confirmed. This strengthens the aforementioned point about the diverse and multi-layered motivations found in web defacements. The reason behind the eventual decline of hacker-to-hacker communication is unknown, yet may be related to the emergence of other, better suited, communication channels. Additionally, as this topic is brought up time and again by defacers, more prosecution might lead to professionalization of the scene, combined with a lessened desire to have a prominent public profile as a hacker.

Interactive incentives motivate web defacers to add in elements addressing other defacers with similar causes, and in some cases might be taken to the point where the entire defacement addresses scene-internal developments. While the greetings element is rather small and can easily be integrated into other incentives, the incentive of hacker-to-hacker communication demands an almost exclusive dedication of the defaced page. As an advantage, they offer a more clearly defined audience and make use of archive sites to increase the lifespan and thus the effect of the message sent.

4.4.6 Solidary incentives

The establishment of group identity in both a positive and a negative way is described in this last incentive. In a positive way, defacers reinforce their belonging to a group with certain values by expressing their compliance with the group's conventions and ethics. Defacers regularly do this by expressing that no harm was done to the original system, as they consider defacements a non-violent form of protest. Often the original site is still available through a link and the admin is given instructions on how to prevent future defacements.

Establishing group identity in a negative way is at times done by leaving a message directed at the perceived enemy. This reinforces one's own (cyber) cultural attribution by stating one's enemies. This can take the form of jokes, threats or insults.

Solidary incentives	**Description**
No harm done	Statement that no harm was done to the target system
Message to the enemy	Message left behind directly addressing the perceived enemy.

Table 4.7: Mapping of solidary incentives onto the research dataset

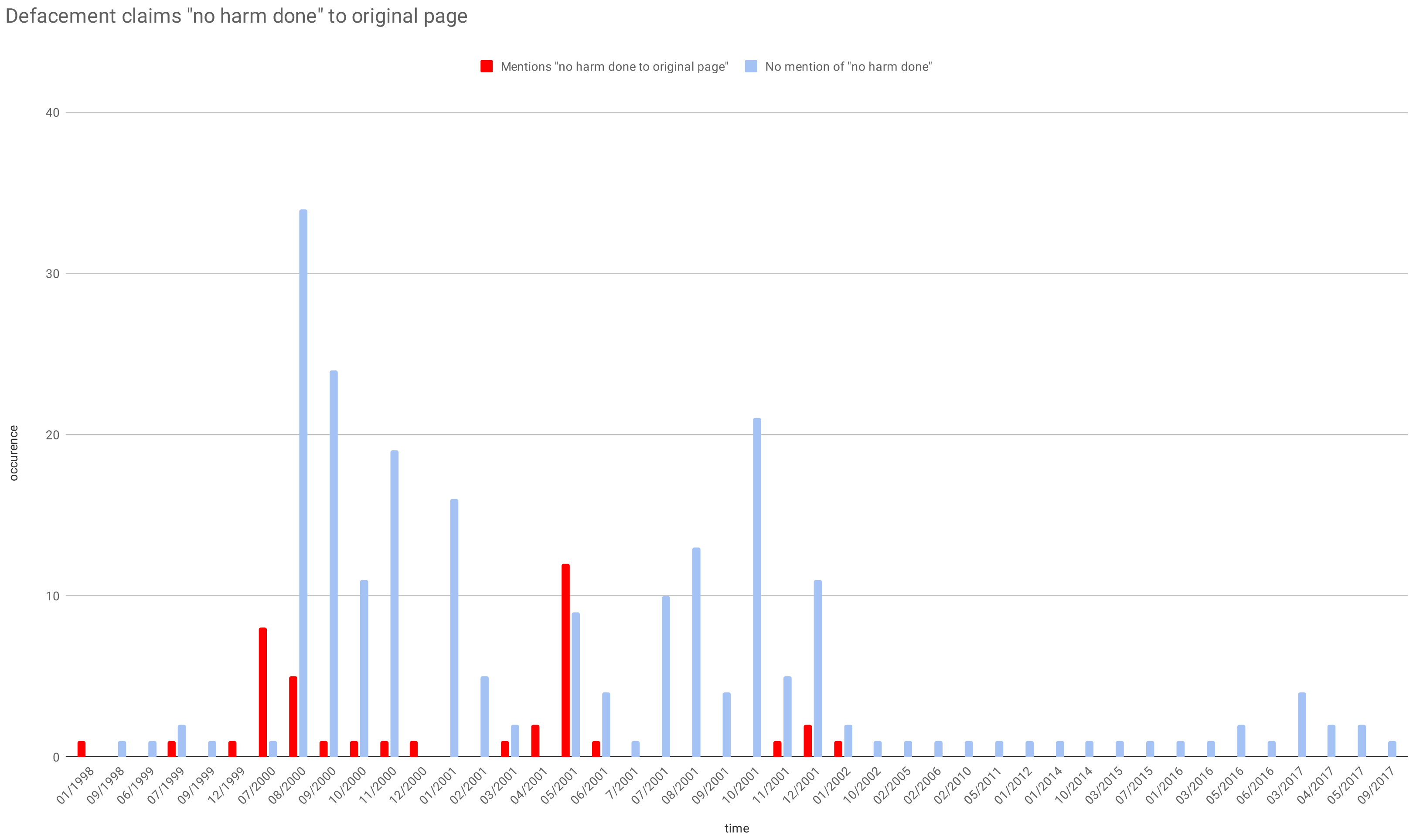


Figure 4.22: Mentions of "no harm done" in defacements

4.4.7 No harm done

Looking at the data, the claim that no harm was done to the target system is mostly found in the time period from 1998 to 2001. During the two activity peaks, mentions of no harm done are less common than in the time leading up to them. The element as a whole disappears after January 2002.

Defacers use the emphasis of being a non-destructive hacker in a dual function. It can serve to communicate a group identity to an outside audience, possibly with the aim to make them aware of a distinction amongst web defacers. Used in that sense, the element can serve to mitigate site owner's frustration over having become a random target in a defacement campaign. To visitors, the mention of no harm – which is often combined with a smug "but you should really learn to secure your server" – also communicates the fact that what they are looking at is the work of a self-aware group with shared values and rules. In that sense, use of the no harm done element works to strengthen public awareness of political web defacements as a form of expression. It is at times combined with an invitation to contact the defacer in order to learn how to prevent further attacks.

Aimed at the scene, the mention of no harm done serves to distinguish oneself from mainstream defacers that aim for high defacement numbers. It is created from the incentive to establish a group identity by publicly embracing the group's values of seeing hacking as creative act. Mentioning that no harm was done to a third party in expressing one's own attitude through hacking is an indirect reference to the Hacker Manifesto. The manifest states "We seek after knowledge... and you call us criminals" (The Mentor 1986). Expressed in the 1986 manifesto is the idea that a hacker's aim is to obtain knowledge and criminalization of hackers stems from ignorance of the true nature of these knowledgeable underdogs.

As an incentive, the element of no harm done primarily has a distinguishing feature, whether it is aimed at surprised site owners, unsuspecting visitors or fellow defacers. It is the expression of a desire to reaffirm a group identity by publicly expressing one's allegiance. The element implies this defacer is pursuing a higher goal and suggests that the means justify the end, especially since allegedly no harm was done to anybody. Defacers using this element are unlikely to be engaged in the form of campaigns that target perceived enemy sites. That the element disappears after 2002 is likely the result of a decline in popularity of the "Information Robin-Hood" image. Having captured it in the dataset nevertheless shows this incentive played an important role for a group of defacers in the key period analysed in this study who felt the desire to distinguish themselves both in communication with their audience as well as towards other hackers.

4.4.8 Message to the enemy

The use of a dedicated message to the enemy in a defacement can serve the need to establish a group identity in a similar way to the public pledge of allegiance seen in the no harm done element. Messages to enemies have a clear addressee (To all you hacker/soldiers of nation X) and work on both external (soldiers) and internal (other hackers) communication. The following figure shows the distribution of said element in the research data set.

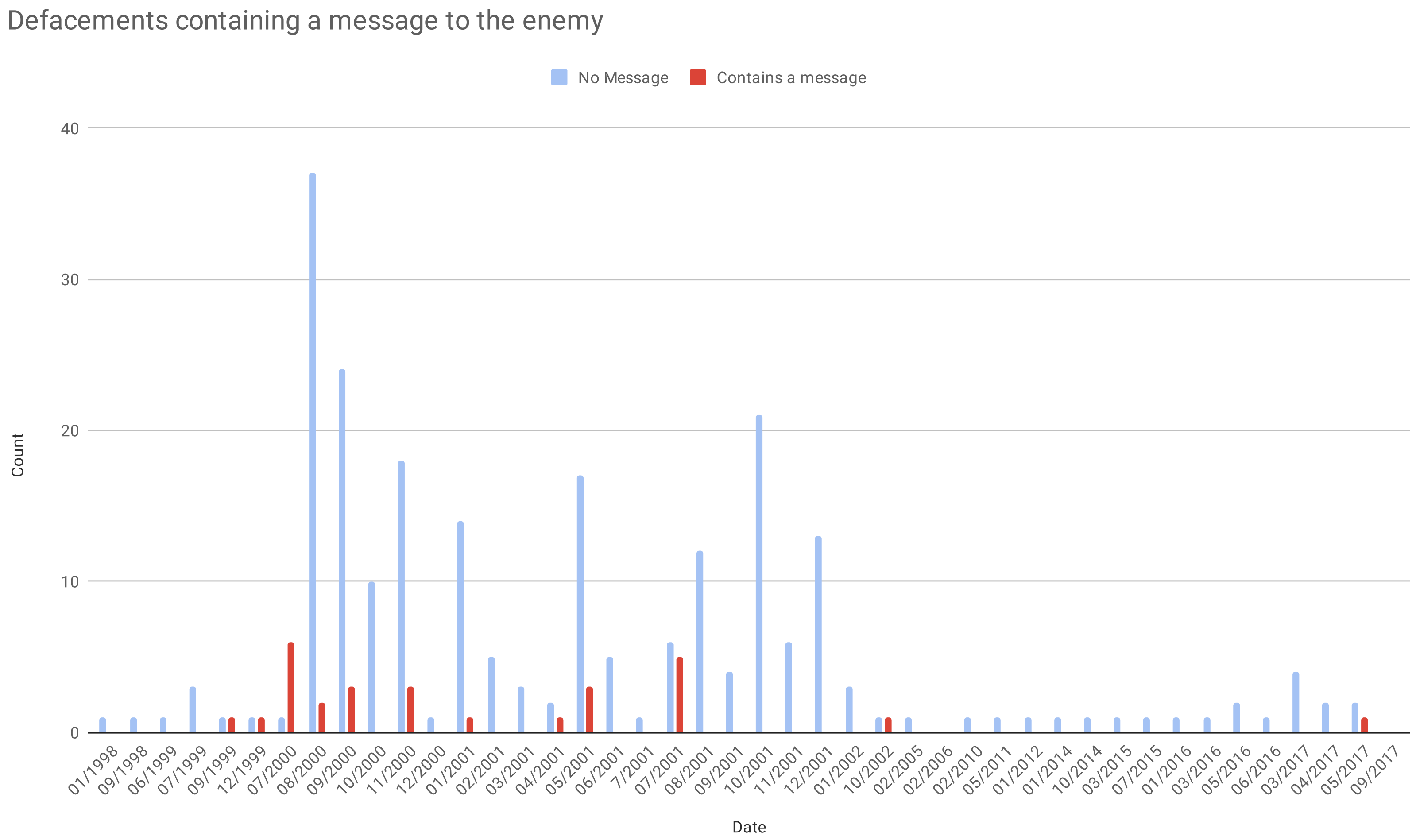


Figure 4.23: Defacements containing a distinct message to an enemy

The data shows that the element of a message to the enemy first occurs in August 1999 and occurs somewhat regularly until July 2001. It is not found in very early defacements and while present in the first activity peak, it is absent in the 9/11 activity peak.

This element is the counterpart to the no harm done pledge described above. Similarly though, it serves to express the author's allegiance to a group by expressing disdain for a shared enemy. It is thus not important for the addressee to receive the message, its primary function lies in the public expression. For an external audience, the messages establish the speaker's identity by aligning them with a political position. Solidarity and group identity are thus constructed by disapproval of the same thing/person/country.

If the element of a message to the enemy is used for more internal communication, it can serve a double function. For an external observer, messages of disapproval of defacers (usually those who prefer quantity over quality) are evidence of a diversity within the scene. These messages also confirm the importance of social interaction within the scene and counter popular notions of hackers as lawless hedonists. For an internal observer, these messages can be part of a meta-game which has been mentioned in the hacker-to-hacker communication section. The meta-game are defacements about the practice of defacing and which actors, targets and negotiate ethical guidelines hackers should follow. This can go as far as whole defacements dedicated to a message for other hackers, using the page exclusively for scene-internal communication.

Messages to the enemy are hard to send when the perceived enemy does not have a clear profile and much less an online presence. Many defacements in the 9/11 cluster for example reference Al-Qaeda, but do not dedicate a separate message. Short expressions of disdain may also be found in the footer section of defaced pages, where the greetings are complemented by a list of people the author dislikes.

The analysis of both solidary incentives – hacker-to-hacker communication and messages to the enemy – shows a strong desire to be part of and reaffirm ties to a specific group. Defacers do this in a positive way by confirming their compliance to scene-internal ethics, or in a negative way by addressing a shared enemy. Both incentives work internally as well as externally in that they inform 3rd-party visitors of the defacements while also contributing to a meta-discussion of the practice of web defacements. The reasons for the decline in use of solidary incentives is unclear. Interactive incentives can be so important for defacers that parts or whole of a defacement are dedicated to messages to other hackers. These meta-defacements then are scene-internal messages. Rarely found – partially owed to the political scope of the data set – these defacements are evidence of high interactivity.

The solidary incentive, the desire to belong to and express belonging to a group, finally was traced through the claims that no harm was done to the original page in the process of defacing. This statement is used to position the speaker in a tradition of non-destructive hacking as expressed in the hacker manifesto and distinguishes those defacing for a higher cause from other, more destructive actors within the scene. This feature is found in the earliest defacement from 1998 up until 2002 and indicates a branch of defacers interested in expressing allegiance to a school of hacking by publicly accepting its rules and standards. Solidary incentives can also be met by publicly expressing disdain for a shared enemy, thus constructing a group identity through exclusion. In defacements, this can be realized through a specific message to the enemy. This feature appears in clusters during both activity peaks.

4.4.9 Motivations: conclusion

The analysis has shown that defacer motivation is diverse and multi-layered. Possible incentives were described and mapped onto the research dataset. Where fruitful, incentive combinations and incentives over time were analysed. While some incentives were represented through categories, others were represented through a combination of binary values. It is not possible to generalize one singular core of defacer motivation, however general characteristics of defacer motivation are as follows:

Web defacements are expressive media. Looking at ends-oriented incentives, what combines defacements across the research data set is the desire to communicate a message to a more or less specified audience. There are two distinct approaches to this. One is the provision of information (whether true or false) without an explicit argument following from it. These defacements appeal to what is assumed to be a sympathetic public with shared values. Other types of defacements use information to develop arguments, accusations, demands and the like. Their function is to develop communicative frames which influence perception far beyond the single incident described in the defacement. This latter type eventually becomes more widespread and partially replaces the mere provisioning of information.

Incentives to be expressive in a certain field were, in the absence of primary data, deduced from the fields of expressions in the dataset. The two most widespread types were the broad category of political expression, followed by defacements explicitly referring to human rights, human rights violations and appeals to various institutions to not allow humans to be denied their human rights. These two types appear throughout the research data set. Other types which appear only occasionally are expressions relating to laws and their application and defacements relating to territorial conflicts.

The desire to interact with others is a strong motivation and usually occurs in combination with one or more of the other described incentives. Tracing the use of greetings in defacements, it was shown that interactive incentives are found throughout most of the research data set, although their use is declining post 2001. The use of greetings also suggests a self-aware and somewhat stable community around defacements.

All of the described incentives appear in combination and fluctuate over time. They are evidence of different strains of defacements and different reactions to world politics. In the scope of development over time, it can be observed how the incentive to provide information, the incentive to express belonging to a certain class of defacers and the desire to interact with other defacers become less. In their place appears an incentive to develop general arguments and frames from smaller pieces of information. This development has its breakthrough with 9/11 and the rise of the memorial type of defacement. With this change also comes a decline of internal communication through defacements as, interacting through greetings and hacker-to-hacker communication becomes less common.

Taking 9/11 as a turning point for web defacements, it can be said that pre-9/11 defacements provide information, reliant on an sympathetic public sphere with shared values to evaluate said information and eventually arrive at the defacer’s political standpoint. A defacer’s profile here is important as it adds to the recognizability and reliability of information. Post 9/11, defacements still provide information, but now they are more likely to develop arguments from smaller pieces of information. Their goal is no longer information provision, but the replication of arguments, sentiments and affective narratives. As part of this development, defacements become shorter, more focussed and as part of a professionalization process featuring less scene-internal chatter.

The overall results explored in this chapter also show that two distinct peaks in defacer activity exist around the first half of the year 2000 and during October 2001. The analysis of tokens and token combinations has identified Kashmir and the 9/11 attacks as some of the most prominent topics during these two peaks. The following two chapters are thus going to explore these two clusters in more detail using forms of textual and semiotic analysis. What the results of this chapter also show is a change in the form and possibly in the communicative function of defacements, seen in the use of greetings and the hacker-to-hacker communication. The two following case studies will thus place a special emphasis on traces and emblematic examples of this change.

5. Case Study 1 – The Kashmir Conflict

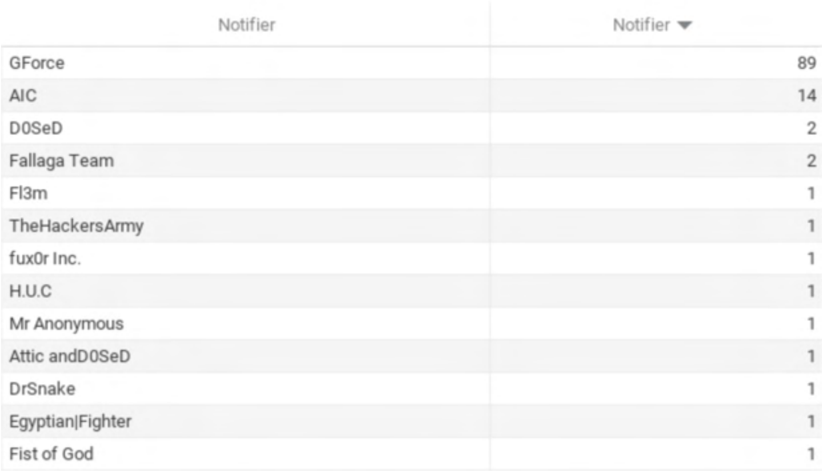
5.1 Introduction

The Kashmir conflict is a territorial dispute between India, Pakistan and China over the Kashmir region. The conflict arose from the 1947 partition of India and has, with varying intensity, continued until today.[37] This ongoing violent conflict has left its marks in the cultural history of Pakistan and India. It has also led to an ongoing cyber war between the two countries, a part of which features web defacements. The selected set of defacements consists of in-scope material relating to the Kashmir conflict. Most defacements are from 1999 to 2002 with some outliers. The temporal distribution of material reflects the scraping process' emphasis on defacements up to 9/11. The topic has been selected since it was a dominant theme within the research dataset (as described in Chapter 4) but also because it features many emblematic elements of web defacements used as a tool in political communication. The following will give an overview of this subsection of defacements.

In total, 116 defacements related to the Kashmir conflict were identified in the data set. The requirement for formulation of this subset was for defacements to have a clear relation to Kashmir, usually by making it the main topic. Especially in post-2001 defacements, declarations of solidarity with Kashmir and other conflict zones are also found in defacements which do not have a clear main topic. These defacements have also been included, as long as they clearly referenced Kashmir. Some of the selected defacement features the names and/or images of victims of violence and war. In accordance with the research ethics statement, identifiable information has been removed from the illustrations used in this and the next chapter.

A total of 13 individual defacer groups have been identified in this cluster:

[37] For a general history of the region and conflict, see Parashar (2018); V. Schofield (2010); Bhat (2019). For the role of digital communication in the conflict, see Gul, Ahmad Shah, and Ahmad (2014); Bunt (2003).



Notifier	Notifier ▾
GForce	89
AIC	14
D0SeD	2
Fallaga Team	2
Fl3m	1
TheHackersArmy	1
fux0r Inc.	1
H.U.C	1
Mr Anonymous	1
Attic andD0SeD	1
DrSnake	1
Egyptian|Fighter	1
Fist of God	1

Table 5.1: Distribution of Notifiers, spelling normalized

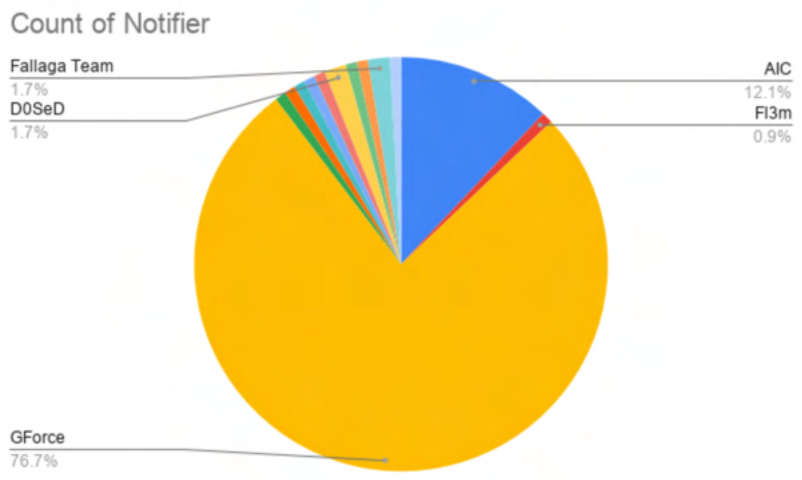


Figure 5.1: Visualization of the above table

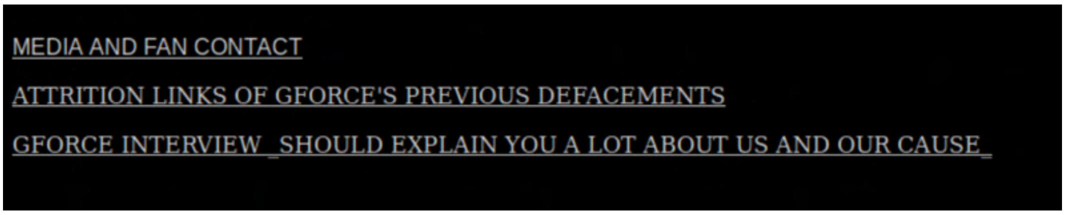
One group, GForce, clearly dominates the field with 89 out of 116 defacements. The second group, AIC, only submitted 14 defacements. All other 11 groups have between one and two defacements. The spelling of group names was normalized in two cases where it was clear they referenced the same group. All involved groups can be divided into two distinct categories: groups primarily formed around the India-Pakistan cyber war and more general defacement groups. The main difference is that the first exclusively submit defacements around their main topic, while the latter might reference Kashmir without having the topic as a clear focus. This also explains the disproportionate division of notifiers. The top two groups will be introduced in the following.

It is noteworthy how one-sided this so-called cyber war is in relation to defacements. The two main actors, AIC and GForce, both are clearly writing from a pro-Pakistan perspective. The rest varies between anti-India and more or less neutral calls for peace. This disproportionate distribution might be related to the trope of the knowledgeable outsider (since the disputed part is politically Indian territory). The knowledgeable outsider trope feeds off the experience of seeing what the mainstream chooses to not see.

As I argue that hacking as a kind of engagement with technology is more appealing for those who see themselves as excluded from a public discourse and thus are trying to break into it to spread their message, it is no surprise that the less-featured Pakistani side in the Kashmir conflict feels the need to utilize web defacements. Hacking in this context provides agency to disempowered voices in discourse. It is at the same time a sort of betting on future developments where, in order to maintain the knowledgeable outsider role, marginalized perspectives are taken up in the hope of eventually receiving recognition. There is only one defacement in the whole set critical of Pakistani influence in the region. This outlier will be analysed in more detail below, not only for its unique political position, but for its advanced communicative strategy.

5.1.1 Groups: GForce Pakistan

GForce (sometimes called Geforce Pakistan) is a hacker collective mostly active in the Pakistan-India cyber war. It is one of the major groups contributing defacements to the Kashmir topic. The group is recognized as “one of the most prominent (group of) hackers to emerge from Pakistan, along with Doctor Nuker and associates in the Pakistani Hackerz Club” (Bunt 2003, 53). Like many groups of the time, GForce offers contact information on many of their defacements:



MEDIA AND FAN CONTACT

ATTRITION LINKS OF GFORCE'S PREVIOUS DEFACEMENTS

GFORCE INTERVIEW _SHOULD EXPLAIN YOU A LOT ABOUT US AND OUR CAUSE_

Figure 5.3: Contact and further reading on a defaced page, DefacementId 8867

The contact information section offers rich reading in terms of defacers using defacement archives to document their work and build a reputation. This is shown by GForce referring visitors to this defacement to an archive of their previous work.

While attrition’s defacement archive was closed for public access until recently, the interview links to the personal site of Srijith Nair, a computer scientist working in IT security. His project *India Cracked* was launched in 2000 to document hacking of Indian sites.[38] The interview, together with two more short self-presentations, can be found on GForce's archived homepage.[39] This gives a

[38] https://web.archive.org/web/20040607174935/http://www.srijith.net/indiacracked/about.shtml

[39] https://web.archive.org/web/20010813193709/http://gforcep.addr.com/interviews.htm

unique insight into the self-presentation of a political hacking group of the time. All three interviews ask about the group's motivation behind the hacks, and all are answered in a similar way. The following is an excerpt from an email-based interview with an unknown publication referred to as *Arab Magazine*.[40]

> >> 1-To start.. why are you doing this?
>
> We are doing this to raise public awareness about the Kashmir issue, and how the Kashmiri Muslims (men, women and children), are, at this very moment, being brutally killed by Indian soldiers and no one in the world is doing anything to stop them. [...]
>
> >> 2-How do you describe yourselves (Hackers, Hacktivists, Freedom Fighters, Mujahideen..)?
>
> We are simply showing the world what is really going on, the truth, which has been manipulated so much by the western media, and because we express our thoughts in a different way, doesn't make us any different from anyone who has ever spoken out to tell the truth. Because we deface websites to do this, I believe the popular term to describe us has become "Hacktivists". (GForce Pakistan n.d.)

The Arab Magazine interview tends to have longer responses than the other two IRC-based interviews. The content of all three interviews is largely similar though. One interview states the number of members to be eight, another mentions six names (the homepage also lists six members) so that some fluctuation in membership can be assumed. Srijith Nair asked the group about their offline identities and got the response that "Most of us [GForce] are students, some of us have pursued jobs in the IT industry" (GForce Pakistan n.d.).

While most of the questions are unchallenging and answers have to be taken with some grains of salt, the noteworthy aspect of them is the insight they give into how the group sees itself. One part of that is understanding hacking as a means towards an end rather than an end in itself:

> When we intrude into systems to make our statements, we do not harm/delete/view any of the data on the system, as we are only there for the purpose of raising global awareness. [When asked about hacking practices] (GForce Pakistan n.d.)

This confirms findings from the previous data analysis chapter about defacers expressing their allegiance to a common cause by publicly referring to a set of common rules – in this case, non-destructive hacking. GForce and other political groups do use hacking to spread their messages, yet they do have an understanding that hacking is simply one of many tools to reach a public as they connect hacking not with destruction but with raising awareness. The conflict between spreading information by occupying online space at the expense of others is expressed in GForce's offer to help affected website owners:

> [Interviewer] Do you help webmaster/admins fix their holes if they ask for your advice/help?

[40] https://web.archive.org/web/20010813174748/http://gforcep.addr.com/arab.txt

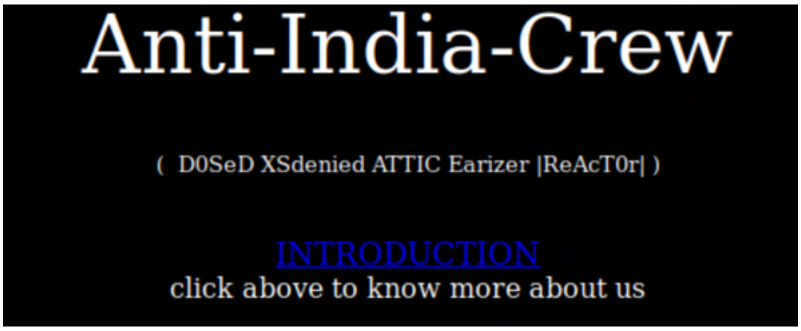
> GF P: Well, not many admins have asked for our help, but those who have, have been helped by us in every way possible to give them advice on how to secure their systems. (GForce Pakistan n.d.)

Finally, relating to the origin of the group’s name:

> GF P: Actually, to be honest I have no clue what the word means. It's just a word. Like aircraft-related high alpha manouvers or something. Sounds cool. (GForce Pakistan n.d.)

5.1.2 Groups: AIC

Anti-India-Crew (AIC, sometimes spelled A-I-C on older defacements) has much less of a public profile than GForce, yet still offers a website for interested readers to find out more about them[41]:



Anti-India-Crew

(D0SeD XSdenied ATTIC Earizer |ReAcT0r|)

INTRODUCTION
click above to know more about us

Figure 5.4: AIC member list and homepage link on a defaced page, DefacementId 8

Similar to GForce’s brand management strategy, AIC also added links to their homepage to defaced pages. The website features a short “about us” text, explaining the motivation and practices of the group:

> The Crew are nice people, well educated and well motivated. All have one goal, to stop the fight between India and Pakistan over Kashmir. So why the hell are we hacking different websites? The answer is simple, to create awareness. The world is becoming smaller with advanced communication and the fastest method of spreading information is the Internet. We do not believe that by killing people we will bring attention and sympathy. That has failed in the past and will fill in the future. Our method is simple, to break into systems and deface their website. No damage is done to the system, nothing is erased. The only think that is changed is the index file. (AIC n.d.)

The self-presentation shows a remarkable similarity to GForce's mission statement, including the practice of not damaging target systems. Both groups express their focus on creating awareness rather than claiming fame in the hacking scene. AIC goes further than GForce in explaining why web defacements are used:

> We have tried everything to gain International Support but to no awail. The United Nations talks alot and plans a lot but does no action. (AIC n.d.)

[41] https://web.archive.org/save/http://www.lordpimp.20m.com/AIC/Main.htm

AIC sees web defacements as one of the few remaining options for creating awareness as public interest turns away from the conflict. Their approach fits into the framework of contesting public memory by overwriting digital text, as AIC's defacements are generally geared towards creating a chronology of events from the Kashmir region. AIC does not provide information on how targets are selected and what kind of exploits are used to gain access to them.

The defaced page in Figure 5.4 lists five members, while the homepage does not go into detail about number or background of the crew. No information is given as to where AIC is based, however as their work expresses obvious Anti-India sentiment, support of Kashmir independence and understanding of Pakistani intervention in the region, it can be speculated that AIC has ties to either Pakistan or Kashmir.

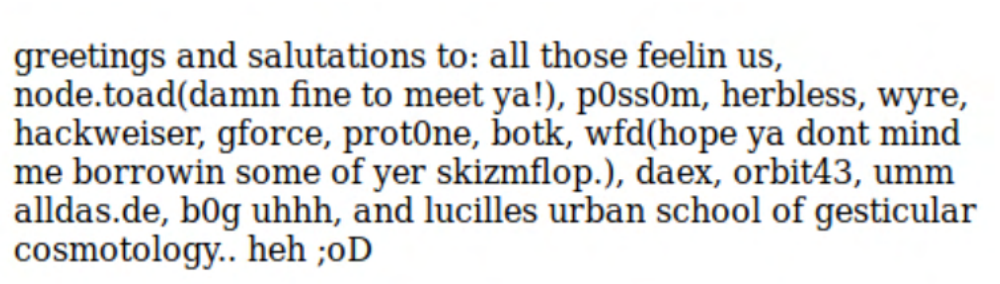
Comparing the efforts invested into public relations between GForce and AIC, it seems that AIC did invest less time and effort into building a stable online presence. The linked homepage is incomplete, links to "history" and "credit" appear in the menu, but there are no actual hyperlinks. This may be related to the group's rather short engagement with the Kashmir issue; while GForce submitted Kashmir-related defacements from July 2000 until October 2001, AIC's active period falls between July and October 2001. What both groups share is a strong focus on information provision as their main strategy. This positions both defacer groups within classic ideas about the public sphere as a place of rational exchange:

> The notion of the political public sphere centered on the idea that private persons might come together through reasoned communication to consider public issues and inform public policy. Because the parties would be well-formed individual persons, and because their discourse would be both rational and critical, the resulting public opinion would be a productive resource for guiding society, not the lowest common denominator of popular passions. [...] At least ideally, it also provided participants with a means of overcoming the differences of status that otherwise divided them and made their opinions sectional rather than truly public. (Calhoun 2010, 3)

The information provided by the defacers has as its goal a contribution to the formation of well-informed individuals capable of partaking in political discussion in the public sphere. Speaking from the outside, through the unconventional medium of defaced web pages, defacers also attempt to overcome divisions and marginalization through their technical expertise. They struggle because their experience is one of not being heard, despite attempts to participate in the public sphere.

5.1.3 Inter-group relations and solidarity

Despite using different communicative styles, both groups clearly state their political allegiance and their relation to other defacers through the taking of a position on the Kashmir conflict. There is a general consensus amongst defacers to oppose India's politics in relation to Kashmir, however that is as far as consensus usually goes. Greetings are a common element in defacements, as Figure 5.5 illustrates.

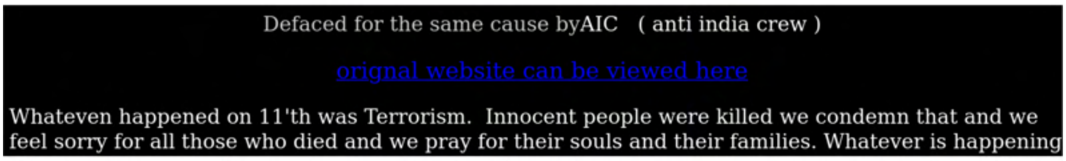


greetings and salutations to: all those feelin us,
node.toad(damn fine to meet ya!), p0ss0m, herbless, wyre,
hackweiser, gforce, prot0ne, botk, wfd(hope ya dont mind
me borrowin some of yer skizmflop.), daex, orbit43, umm
alldas.de, b0g uhhh, and lucilles urban school of gesticular
cosmotology.. heh ;oD

Figure 5.5: Greetings on a defaced page showing the author met and worked with some of the other groups, DefacementId 8655

Inter-defacer relations are important since, beyond the usual banter and rivalry, they show that the authors are aware of similar work going on at the time and that they have cooperated and interacted with other groups. Figure 5.5 shows a defacer named fux0r Inc. sending his regards to other defacers. On the original page, he begins with "Much luv to GforcePakistan" before the broadcast message. It is especially interesting since it shows that not only did he meet and interact with at least two of the mentioned individuals/groups, but the timing of these greetings is also significant. The defacement featuring the above message was captured on the 9th March 2001, after GForce's activity had practically ceased. While the group had defaced websites from July 2000 to March 2001, there are only two Kashmir-related defacements by GForce after fux0r Inc. send his love. This hints at two things; that the author knew the recent history of web defacements up until that point in March 2001 and knew who the main actors in the field of political defacements were, hence his regards to other defacers and alldas.de, a cybercrime archive. The timing also suggests the possibility that fux0r knew of GForce's withdrawal and felt the need to honour their work.

The example represents one part of a three-part page design found in many defacements. Typically, a header and footer frame the message, each of the three having a distinct function. The header is commonly used to introduce the defacer, sometimes featuring a slogan or quote. After the message, the footer is used to refer to other people within the scene, be it positively (greetings, shout outs) or negatively (sometimes lists of disliked groups/individuals). The use of a special lingo, especially aberrant spelling, is commonly limited to header and footer. This indicates that these two elements target an audience of fellow defacers while the message in the body is commonly kept in more standard English suggesting a more general audience.



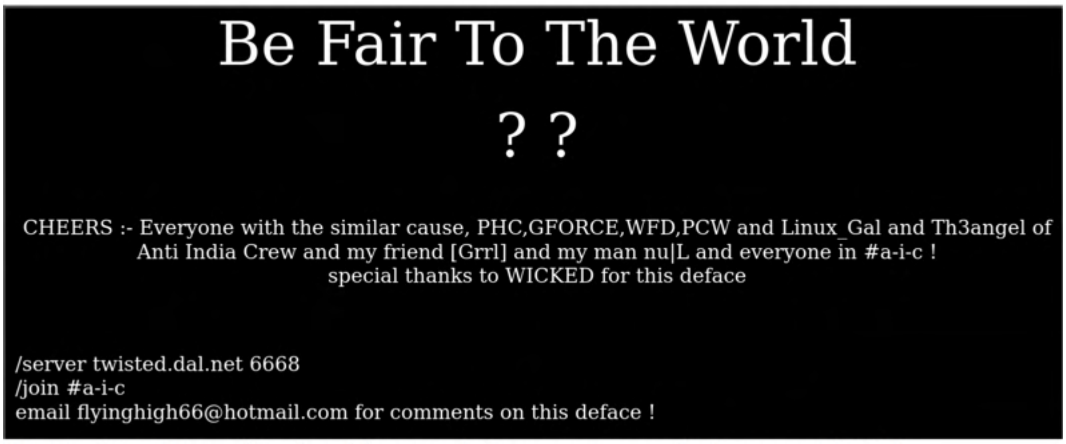
Defaced for the same cause byAIC (anti india crew)

orignal website can be viewed here

Whateven happened on 11'th was Terrorism. Innocent people were killed we condemn that and we feel sorry for all those who died and we pray for their souls and their families. Whatever is happening

Figure 5.6: Header and part of body of a defaced page, DefacementId 381

This defacement features a link to the original site, implying that the attacker did not intent delete the original site.



Be Fair To The World

? ?

CHEERS :- Everyone with the similar cause, PHC,GFORCE,WFD,PCW and Linux_Gal and Th3angel of Anti India Crew and my friend [Grrl] and my man nu|L and everyone in #a-i-c !
special thanks to WICKED for this deface

/server twisted.dal.net 6668
/join #a-i-c
email flyinghigh66@hotmail.com for comments on this deface !

Figure 5.7: Part of body of footer of the same page, DefacementId 381

Greetings are posted in the footer and visitors are invited to contact the defacer group.

While much of this remains speculation at this point, it can be assumed that members and groups within the defacement scene were well aware of one another and that contacts were established. It further serves as proof for the thesis that cybercrime archive sites such as alldas.de or Zone-H were gathering points for the scene rather than information pools for the general public. The knowledge of and familiarity with content and lingo, together with rules and etiquette – it is considered very offensive to re-deface a defacement, overwriting another hacker's work – act as a signifier of membership within the community. Gabriella Coleman identified similar mechanisms in her work on the imageboard 4chan:

> much of the material is designed to be shocking to outsiders, a discursively constructed border fence meant to keep the uninitiated—aka "n00bs" or "newfags"—far, far away. (Nearly every category of person, from old-timers to new-timers, is labelled a "fag." On 4chan, it is both an insult and term of endearment. We will see the suffix many times in this book.) For insiders, it is the normal state of affairs, and one of the board's defining and appealing qualities. (Coleman 2014, 42)

While shocking material is less of a defining feature of web defacements than it is on 4chan and similar imageboards, the idea of a "discursively constructed border fence" applies to the communications within the hacking scene as well. It shows a certain kind of familiarity as well as keeping the uninitiated away. Additionally, the use of any shocking material is a precaution against the usurpation of material by the mainstream media who are by conventions and regulations unable to broadcast such material.

But the incompatibility Coleman describes here extends only on the level of content. It is also a semantic incompatibility whereby mainstream media stands for the use of the classic triangular semiotic relationship between Symbol, Reference and Referent (Ogden and Richards 1985, 11). In contrast to this, the communication described by Coleman and most of the communication in web defacements uses symbols as stimuli to generate responses. The actual message, if it exists, is obscured by a layer of “noise” in the form of referent-less symbols. In individual cases, this can be harmless trolling, provocation or – as mentioned – a useful border fence keeping out the uninitiated. On a larger scale, this deliberate abandonment of semiotic relation means to flood a communication network with symbols which, for the outside observer, lead nowhere. The result of this can be to desensitize the network to certain omnipresent stimuli, until that stimuli becomes powerful enough to again manifest itself as an actual reference – that case can be made for the “ironic” use of anti-minority sentiment. Eventually, this strategy leads to a crisis of trust within the communication network when symbols can no longer with reasonable certainty be assumed to stand in for a certain referent, or any referent at all. These two, essentially incompatible communication models are the caveat of web defacers: what they want to communicate outwards is obscured by how they communicate their message. It is as if 4chan wrote a letter to the White House.

The uniformity of opinions in the captured defacements is the remnant of an online community with its own social rules, conventions, cues, hierarchies and conflicts. The importance of community building in a text-based online environment has been stressed by Baym:

> Social cues, create immediacy, entertain, and show off for one another, they build identities for themselves, build interpersonal relationships, and create social contexts [...] Performing well can bring a person recognition, or at least lead to a sense that there is a real person behind otherwise anonymous text. (Baym 2010, 61)

As initially stated, political opinion usually only varies between anti-India sentiment specifically and a general call for peace in the region implying Indian retreat from Kashmir. While the two big groups dominate the thematic collection here – and both have clear anti-Indian agendas – even amongst defacers only represented by a single defacement there is little dissent and no debate about who is at fault and how the situation may be relieved. This fact, together with a statement given by GForce stating that so far they have not received any counter-attacks but expect them[42], shows how dominant this particular value system was in the cyberwar of the early 2000s.

A final aspect in term of relations within the scene are defacements unrelated to Kashmir, but containing references to the conflict. For example, a number of defacements referring to Gaza feature a “solidarity” section where the struggle in Kashmir is mentioned. A total of six such defacements have been identified in the data set.

5.2 Content and seriality

Analysis of defaced pages is aided by a systematic coding of defacement types. As this study focusses on a defacement’s communicative function, material was coded by substantive topic where possible. Where it was not possible to identify a clear main topic, material was added to groups 3 (Background), 11 (unrelated reference) and other/mixed. There is generally little overlap between categories so that the majority of defacements can be clearly assigned one of the categories.

1 Reports of torture – defacements in this category are part of a series authored by AIC. Defacements give details about torture methods and locations.

2 US/UN appeal – defacements in this category are mostly part of a series of defacements authored by GForce. They all are centred around a direct appeal to United Nations or the United States to get involved in Kashmir. Defacement 8986 discussed below is part of that series.

3 Background information – defacements in this category give general information on Kashmir and the ongoing conflict. They do not usually feature any direct call to action.

4 ISI article – defacements in this category speak out against the involvement of Pakistani security agency ISI in the escalation of the Kashmir conflict. DefacementId 8190 is the only known defacement in this category.

5 Context – this category is used to describe all defacements that cannot be clearly assigned to one of the other categories. Defacements in this category feature a short piece of text contextualizing the situation in Kashmir within a larger geopolitical context.

6 POV report – defacements in this category feature texts which are marked as the objective viewpoint of an unnamed speaker. They describe

[42] [Interviewer] Have you suffered any counter attacks? - Not yet, but we expect a few shortly (GForce Pakistan n.d.)
It is unclear here if what is referred to are attacks from other hackers or what later has become known as a hack back or active cyber defence (Lin 2016, 3) – usually implying the involvement of a security agency.

different events but their common feature is that they are determined by this first-person-narrative.

7 News about incidents – defacements in this category list specific incidents related to the conflict. They usually are taken from a news source or written in the style of a news ticker.

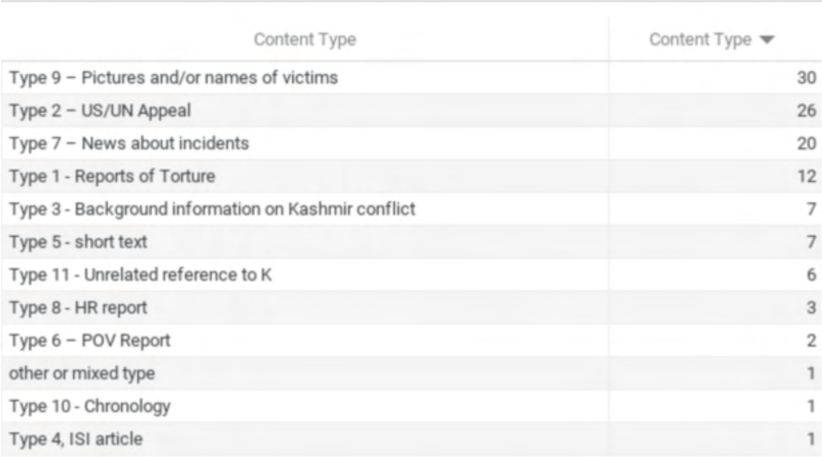
8 Human rights report – defacements in this category refer to a human rights case study done by Amnesty International in March 1997.

9 Pictures and/or names of victims – defacements in this category use graphic pictures to accuse India of excessive brutality. This is sometimes amplified by adding the names of victims and giving context of their death.

10 Chronology – defacements in this category give a chronology of the conflict. They do not contextualize as much as type 3.

11 Unrelated reference to Kashmir – this category contains all defacements that are not primarily concerned with Kashmir, but feature a reference to it. Usually this is in an expression of solidarity with the Muslim population.

12 Other/mixed type – defacements which can not clearly be aligned with one of the other categories, mostly for the lack of a clear topic.



Content Type	Content Type ▼
Type 9 – Pictures and/or names of victims	30
Type 2 – US/UN Appeal	26
Type 7 – News about incidents	20
Type 1 - Reports of Torture	12
Type 3 - Background information on Kashmir conflict	7
Type 5 - short text	7
Type 11 - Unrelated reference to K	6
Type 8 - HR report	3
Type 6 – POV Report	2
other or mixed type	1
Type 10 - Chronology	1
Type 4, ISI article	1

Table 5.2: Distribution of content type, excluding other/mixed

The distribution of content shows a clear focus of defacers on human rights violation as types 9,7 and 1 would be used to disseminate information on these actions. While some of these types are more focussed on providing the information and remembering the victims of atrocities, type 2 usually derives the urgency of its appeal from reported human rights violations.

The distribution of types is representative of the scope of the data collection. It shows that defacements function by overwriting electronic text with the intention to insert information, often images, into circulation. In doing so, defacers establish a counter-public based on a shared discourse by directly addressing people who are part of that discourse (Warner 2010, 55). In reading and engaging with the defacement, users involuntarily become part of a public created by the text, even if only for a moment:

> Fundamentally mediated by public forms, counterpublics incorporate the personal/impersonal address and expansive estrangement of public speech as the condition of their own common world. Perhaps nothing demonstrates the fundamental importance of discursive publics in the modern social imaginary more than this—that even the counterpublics that challenge modernity’s social hierarchy of faculties do so by projecting the space of discursive circulation among strangers as a social entity, and in doing so fashion their own subjectivities around the requirements of public circulation and stranger-sociability. (Warner 2010, 87)

What Warner describes as personal/impersonal address is especially important for defacements and needs to be kept in mind when targets and potential audiences are discussed. Defacements can choose their audience somewhat by selecting target URLs, yet largely defacers have little control over who their audience is going to be. This special situation of creating a public through discursive circulation, yet with an unclear audience and monodirectional communication creates a situation defacers have to negotiate using different argumentative styles which are reflected in the described types.

It further shows that there is a split in the argumentative approach used, with some types presenting rational arguments which then lead up to a conclusion or a call to action (see DefacementId 8986 as an example of that strategy), whereas types 9, 1 and 8 rely on the effect that said information is going to have on the reader. With this split comes varying emphasis of the speaker role assumed by the defacer. Speaker roles (and types, for that matter) generally follow modes of discourse which are narration, description, exposition, and argumentation (Baldick 2004). While almost all defacers seem to enjoy a bit of publicity and feature their name prominently on the defaced page, the more of an argument is made, the more the speaker role needs to be defined to authorize or warrant the content. This can go as far as using strategies of branding, such as a recognizable look of pages defaced by a certain group (AIC), but it also includes featuring links to a homepage on each defacement, as is the case with GForce and many other defacers.

The more the attempt to influence public discourse is reliant on the power of information to speak for itself rather than argumentative persuasion, the less a need for a well-defined speaker role exists since the argument is made not by the speaker, but by the audience through shared moral values. Some branding still applies throughout, but defacements build around type 9 (pictures and names of victims) generally are centred around that information and do not spend a considerable amount of time establishing the legitimacy of the speaker. Such calls to pathos are mechanisms to circumvent a lack of cultural capital as brought about by social differences (Calhoun 2010, 21).

In addition to the described two strategies (making an argument vs providing information), there exists a third type of strategy. This strategy is a recourse to sentimental writing, realized in types 6 (First-person-accounts) and in some instances of type 1 texts. Sentimentalism is mentioned here as a phenomenon which has been discussed in relation to the formation of democratic processes, especially in relation to the USA. Assessment of sentimentalism ranges from applying a general sentimentality to American democracy from the moment of independence on (Burstein 1999, 5), to the more middle-class based escapism from politics which Mary Louise Kete (2000) describes. At least an equal amount of research is available on the literary consequences of sentimentalism, again ranging from understanding the "sympathetic state" as prototypical for the democratic state (Barnes 1997, 2) to Ann Douglas' well- known *The Feminization of American Culture* (1988). Despite the diverging opinions on the outcome of the sentimental tradition in American fiction, even Jane Tompkins (1985) and Douglas (1988) agree that sentimental writing is an attractive vehicle for otherwise marginalized voices to make themselves heard in the American public. In a translation from American fiction to web defacements written in English, featuring appeals to US institutions, this strain of sentimentalist writing can be seen as a third communicative strategy aside the argumentative and informative approach. A sentimental approach is used to bridge cultural differences with the aim to form an empathetic public, which is formed through a shared emotional response. When this approach is used, the attempt to influence public debate becomes an attempt to influence public attitude and emotions, with the depicted information serving as emblematic prototypes. Influence in this case comes from affective intensities as much as informational quality. It can be argued that the sentimentalist approach is important for its universal appeal, bypassing the need to exhaust the reader with long histories of the topic at hand before coming to the call to action. This shift towards a more sympathetic approach in defacements will surface again in the discussion of 9/11 related defacements. Until then, it will remain a small subgenre in the research data set.

5.3 Seriality

Table 5.2 above suggests a strong formal resemblance between texts of the same category, however this is not always the case and great variation of the theme can be found in most categories. Most noteworthy in terms of reusing the exact same text is AIC who, in all their defacements, have a clear focus on type 1 texts (reports of torture) and use parts or all of a text also featured on their home page. Since the group consists of multiple members working independently, the use of these text snippets suggests some level of coordination and agreement between members. The decision to use pre-fabricated text pieces is likely also due to the increase production rate seriality allows for. Copy and paste is of course much quicker than formulating new texts for each individual site. In some cases, an attacker obtains access to a server hosting a range of individual websites. In a so-called mass defacement, all of the hosted sites are defaced at once. This practice does not leave much time for individual formulation of narratives.

Relying on an agreed upon corpus, the defacer can hit more pages at the same time. In the example discussed in this chapter (DefacementId 8986), the observed contradictions in style, grammar and context are likely due to the mixed use of text snippets and the individual defacer’s insertions. In the example discussed below, elements that are re-used in many other defacements by the same groups is everything below the line “Our Demands?”. Other groups, mostly because they are not as focussed on one singular topic such as AIC, do not make extensive use of seriality. The content of most defacements in this cluster is individual enough to suggest that at least most of it was written specifically for the occasion.

Where seriality is used is in the context of creating a recognizable brand image for defacers or defacer groups. By using the same footer, individual defacements are brought together as parts of an assemblage where separate arguments lead up to the same conclusion. There also is clear use of seriality in terms of content, especially amongst the two largest groups in the cluster. What was not observed was a re-use of content across groups, neither in an attempt to recognize and honour their work, nor in a defamatory context. While shout-outs are common, groups remain distant when it comes to featuring each other’s work. Amongst hacktivist groups, overwriting another group’s work is seen as highly transgressive. The only exception being text types referring to the same source, mostly type 9 (Pictures and/or names of victims), however this is understood as the result of drawing from the same source rather than re-using someone else’s content.

5.4 Targets and reach

Linking back to previous chapters, where some of this logic is already discussed, the question of how targets are chosen remains. There are generally two paths to choose from. One is to select the easiest targets, the most insecure sites, with the aim of defacing as many sites as possible. The original content and the owner of these pages then is of secondary interest. The second path then is to select targets based on their owner. This may reach from an actual institution, for example the US Justice Department Website[43], down to the top-level domain so that any page ending in .us becomes a target. This approach takes more time and effort but is likely to yield more recognition within the scene. Both approaches can be used in combination, for example government sites might be slow to adapt to new online threats and thus present easy pickings. In the same way, websites might become targets simply because their domain indicates affiliation with the enemy.

In an interview, a member of GForce claims to select targets based on their political affiliation:

[43] The page was defaced following the death of Aaron Swarz, see Zabarenko (2013).

<SugarKing>[Interviewer] some of your defacements are gov servers, any reason of targeting gov's, are you afraid to get busted? [...]

<sniper__>[GForce member] Not really, We are not afraid to get busted for the reason that it's a good cause, secondly members are out of the feds reach ;) [...]

<SugarKing> yeah of course [...]

<SugarKing> you are one of, if not the only, people on attrition that I've seen that actually have a REASON

[…]

<snipah-> US government was targetted because 1) more people view .gov's and we can do a good job in achieving th goal, we are out for. 2) We're a big angry :) [...]

<snipah-> big=bit (GForce Pakistan 2000)

Here the claim is made that .gov sites are attacked deliberately in an attempt to create more awareness as these sites are seen as a good way to reach out to a US audience. In snipah-'s answer, the split between the communicative function of the defacement and the disruptive function of the hack are hinted at when he lists the reasons for targetting US government sites which are more page views and a more targeted expression of anger. Also interesting to note, is the interviewer's remark that GForce is one of the few groups with a reason behind their defacements.

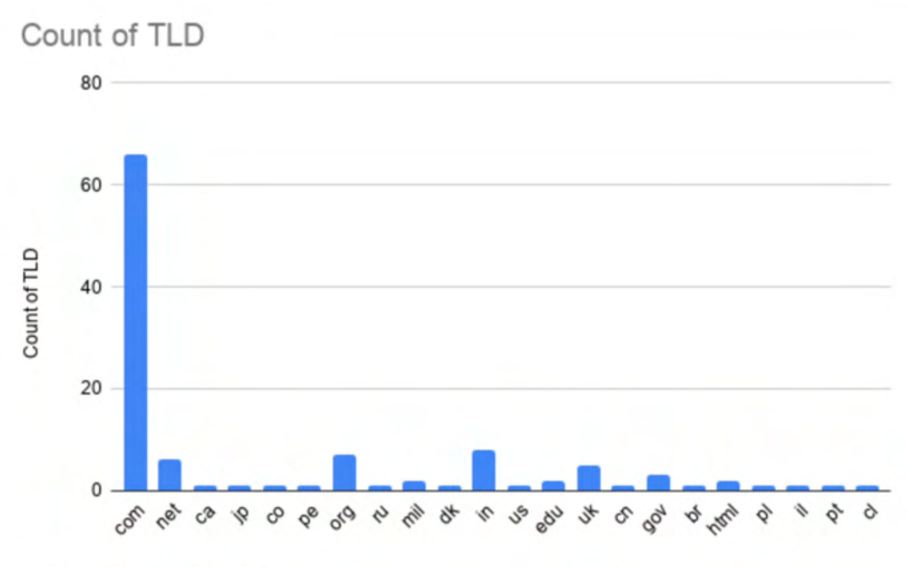
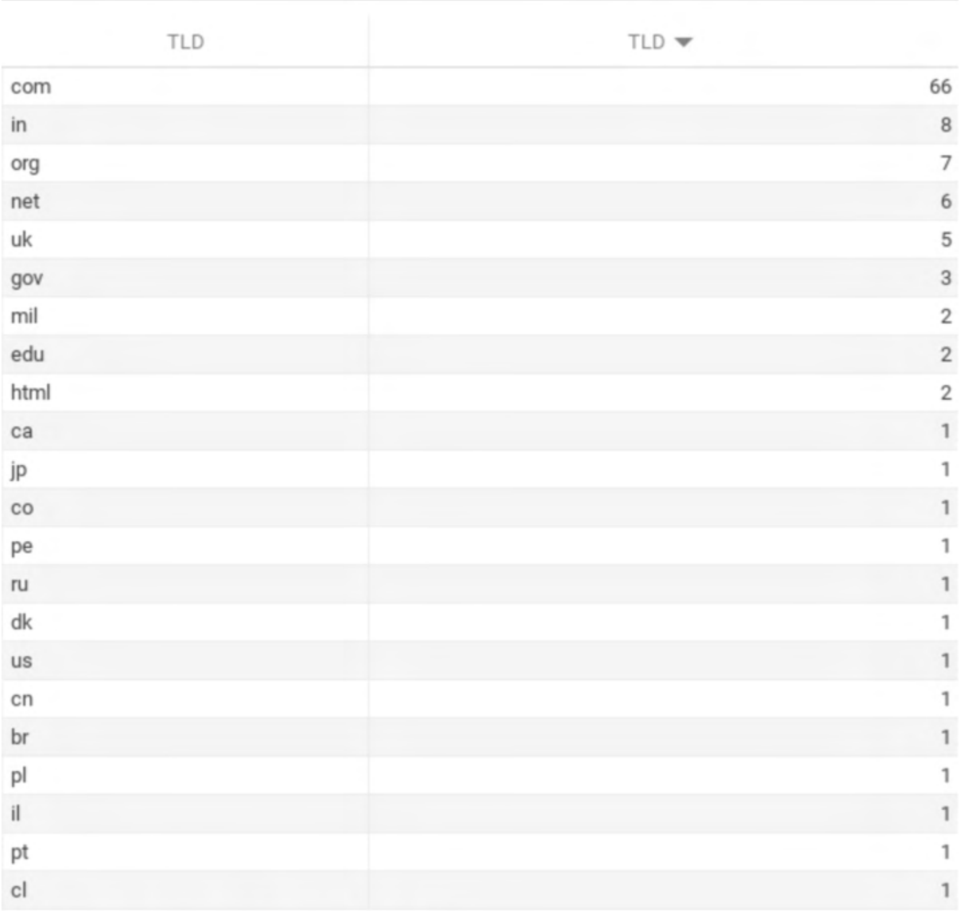


Figure 5.8: Defaced TLD

The following graph breaks down defacements in the Kashmir subset by TLD to further investigate the distribution of targeted web pages:



TLD	TLD ▼
com	66
in	8
org	7
net	6
uk	5
gov	3
mil	2
edu	2
html	2
ca	1
jp	1
co	1
pe	1
ru	1
dk	1
us	1
cn	1
br	1
pl	1
il	1
pt	1
cl	1

Table 5.3: Count of TLDs defaced

The data only partially supports snipah-’s claim. Looking at the count of TLDs[44] of defaced pages within the Kashmir cluster, the vast majority are .com domains. In the sector of generic domains, .com is followed by .org and .net, with .gov (reserved for US government services) and .mil (US military) only accounting for two and three defaced pages respectively. Regarding country-specific TLDs, .in (India) and .uk (United Kingdom) are the two most commonly defaced domains of their kind.

While the data supports the claim that .gov domains were targeted, it shows that the overwhelming majority of defacements happened on the .com domain. As mentioned before, this is indicative of a strategy of generating reach by defacing as much as possible, with target quality being subordinate to target quantity. However, the list of defaced TLDs also acknowledges the existence of a strategy of quality over quantity, with some defacements focussed on prestigious targets such as .gov and .mil domains. It is perhaps of little surprise to see a number of .in domains defaced in the context of this Kashmir cluster. What surprises is more the absence of Pakistani domains (.pk), even though a spread of other country-coded

[44] A Top-Level domain is a domain at the highest level of the Internet's domain name system. Relevant here are country-code tlds (.ie, .ru, .in, etc.) and so-called generic domains such as .com (commercial), .edu (educational) and .gov (US government services) (Postel 1994). For more detail, see Chapter 4.

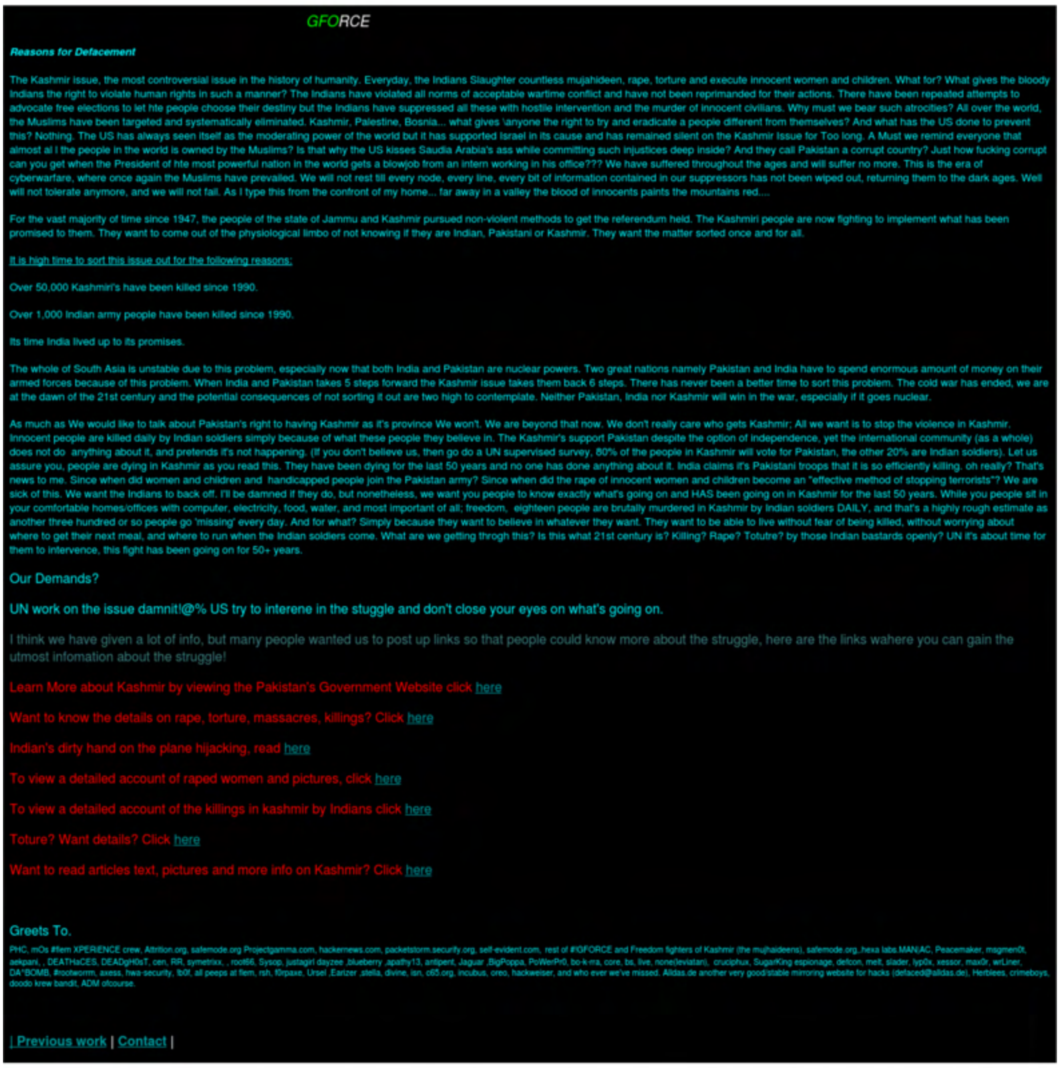
TLDs is seen. This ties in with the earlier observation of how one-sided the archived defacement scene is. While in the following, one anti-Pakistani defacement will be analysed, this represents an outlier within an otherwise surprisingly uniform corpus.

In the interview, snipah- mentions the larger outreach capacity generated by high-value targets such as .gov sites. This is likely to be true, however calculating the outreach capacity for defacements is usually impossible. Unless websites publish historic visitor numbers, sources are virtually non-existent pre-2010. Even if such data were available, it is not possible to determine how long the defacement was online before it got removed. It is in most cases more likely to assume that the defacement received more attention in its archived state than when it was live. It cannot be generally assumed that defacers have had access to information on their target's daily visitor numbers. This lack of information supports the assumption that in the Kashmir cluster, targets were chosen primarily based on their availability.

In the following two defacements that will be examined in close detail, no assumptions about how many people saw the defacement on the original page will be made, since no data exists to base any assumptions on. The two defacements do, however, form an overview of the cluster with one being emblematic of defacements found at the time and the other one being an interesting outlier hinting at the coming professionalization of political defacements.

5.5 8986, communicative strategy

Using the DefacementId 8986 (Figure 5.9) as an example, the key strategies in communication via defaced web pages can be explored. This defacement in its structure is emblematic of most of the defacements surrounding the Kashmir conflict.



GFORCE

Reasons for Defacement

The Kashmir issue, the most controversial issue in the history of humanity. Everyday, the Indians Slaughter countless mujahideen, rape, torture and execute innocent women and children. What for? What gives the bloody Indians the right to violate human rights in such a manner? The Indians have violated all norms of acceptable wartime conflict and have not been reprimanded for their actions. There have been repeated attempts to advocate free elections to let hte people choose their destiny but the Indians have suppressed all these with hostile intervention and the murder of innocent civilians. Why must we bear such atrocities? All over the world, the Muslims have been targeted and systematically eliminated. Kashmir, Palestine, Bosnia... what gives \anyone the right to try and eradicate a people different from themselves? And what has the US done to prevent this? Nothing. The US has always seen itself as the moderating power of the world but it has supported Israel in its cause and has remained silent on the Kashmir Issue for Too long. A Must we remind everyone that almost al l the people in the world is owned by the Muslims? Is that why the US kisses Saudia Arabia's ass while committing such injustices deep inside? And they call Pakistan a corrupt country? Just how fucking corrupt can you get when the President of hte most powerful nation in the world gets a blowjob from an intern working in his office??? We have suffered throughout the ages and will suffer no more. This is the era of cyberwarfare, where once again the Muslims have prevailed. We will not rest till every node, every line, every bit of information contained in our suppressors has not been wiped out, returning them to the dark ages. Well will not tolerate anymore, and we will not fail. As I type this from the confront of my home... far away in a valley the blood of innocents paints the mountains red....

For the vast majority of time since 1947, the people of the state of Jammu and Kashmir pursued non-violent methods to get the referendum held. The Kashmiri people are now fighting to implement what has been promised to them. They want to come out of the physiological limbo of not knowing if they are Indian, Pakistani or Kashmir. They want the matter sorted once and for all.

It is high time to sort this issue out for the following reasons:

Over 50,000 Kashmiri's have been killed since 1990.

Over 1,000 Indian army people have been killed since 1990.

Its time India lived up to its promises.

The whole of South Asia is unstable due to this problem, especially now that both India and Pakistan are nuclear powers. Two great nations namely Pakistan and India have to spend enormous amount of money on their armed forces because of this problem. When India and Pakistan takes 5 steps forward the Kashmir issue takes them back 6 steps. There has never been a better time to sort this problem. The cold war has ended, we are at the dawn of the 21st century and the potential consequences of not sorting it out are two high to contemplate. Neither Pakistan, India nor Kashmir will win in the war, especially if it goes nuclear.

As much as We would like to talk about Pakistan's right to having Kashmir as it's province We won't. We are beyond that now. We don't really care who gets Kashmir; All we want is to stop the violence in Kashmir. Innocent people are killed daily by Indian soldiers simply because of what these people they believe in. The Kashmir's support Pakistan despite the option of independence, yet the international community (as a whole) does not do anything about it, and pretends it's not happening. (If you don't believe us, then go do a UN supervised survey, 80% of the people in Kashmir will vote for Pakistan, the other 20% are Indian soldiers). Let us assure you, people are dying in Kashmir as you read this. They have been dying for the last 50 years and no one has done anything about it. India claims it's Pakistani troops that it is so efficiently killing. oh really? That's news to me. Since when did women and children and handicapped people join the Pakistan army? Since when did the rape of innocent women and children become an "effective method of stopping terrorists"? We are sick of this. We want the Indians to back off. I'll be damned if they do, but nonetheless, we want you people to know exactly what's going on and HAS been going on in Kashmir for the last 50 years. While you people sit in your comfortable homes/offices with computer, electricity, food, water, and most important of all; freedom, eighteen people are brutally murdered in Kashmir by Indian soldiers DAILY, and that's a highly rough estimate as another three hundred or so people go 'missing' every day. And for what? Simply because they want to believe in whatever they want. They want to be able to live without fear of being killed, without worrying about where to get their next meal, and where to run when the Indian soldiers come. What are we getting throgh this? Is this what 21st century is? Killing? Rape? Totutre? by those Indian bastards openly? UN it's about time for them to intervence, this fight has been going on for 50+ years.

Our Demands?

UN work on the issue damnit!@% US try to interene in the stuggle and don't close your eyes on what's going on.

I think we have given a lot of info, but many people wanted us to post up links so that people could know more about the struggle, here are the links wahere you can gain the utmost infomation about the struggle!

Learn More about Kashmir by viewing the Pakistan's Government Website click here

Want to know the details on rape, torture, massacres, killings? Click here

Indian's dirty hand on the plane hijacking, read here

To view a detailed account of raped women and pictures, click here

To view a detailed account of the killings in kashmir by Indians click here

Toture? Want details? Click here

Want to read articles text, pictures and more info on Kashmir? Click here

Greets To.

PHC, mOs #flem XPERIENCE crew, Attrition.org, safemode.org Projectgamma.com, hackernews.com, packetstorm.security.org, self-evident.com, rest of #GFORCE and Freedom fighters of Kashmir (the mujhaideens), safemode.org,.hexa labs.MANIAC, Peacemaker, msgmen0t, aekpani, , DEATHaCES, DEADgH0sT, cen, RR, symetrixx, , root66, Sysop, justagirl dayzee ,blueberry ,apathy13, antipent, Jaguar ,BigPoppa, PoWerPr0, bo-k-rra, core, bs, live, none(leviatan), cruciphux, SugarKing espionage, defcon, melt, slader, lyp0x, xessor, max0r, wrLiner, DA^BOMB, #rootworm, axess, hwa-security, lb0f, all peeps at flem, rsh, f0rpaxe, Ursel ,Earizer ,stella, divine, isn, c65.org, incubus, oreo, hackweiser, and who ever we've missed. Alldas.de another very good/stable mirroring website for hacks (defaced@alldas.de), Herblees, crimeboys, doodo krew bandit, ADM ofcourse.

| Previous work | Contact |

Figure 5.9: Full page screenshot of a page defaced by GForce Pakistan, ID 8986

5.5.1 Background

The page was originally submitted to the alldas.de or attrition.org archive on the 7th of September, 2000 and eventually handed over to Zone-H with the contents of that archive. It could not be determined what the target page was as no valid capture of it exists in the Internet Archive and the domain has since gone offline. The domain ending in usuhs.mil suggesting the target page was affiliated with the

US-American Uniformed Services University and thus mostly serving US visitors. The target page was completely overwritten and no reference to it is made throughout the text.

5.5.2 Structure

The defacement starts with the name of the group responsible, continues on to “reasons for defacement”, then expresses vague demands before closing with a list of links and greetings. By its structure, the page is supposed to be read all the way through, with the highlighted links offering additional reading to substantiate the message. In the monotony of light blue text, only the name GForce and the links are visually emphasized. Looking at the underlying HTML confirms that more work went into the GForce logo than formatting or proofreading of the text[45]. The way the text is framed by the logo and the links to previous work suggests the author was conscious of building a brand image for the group. In fact, this defacement is part of a series of similar works, all framed by this dual reminder of authorship. The structure thus creates a framing of content by the two identifying elements, header and footer, whereby its communicative function is to speak to two communities on two different levels. To function as a part of GForce's reputation as a capable hacking group, the defacement needs to be clearly attributed to them, hence the need to feature the group name prominently. To function as a political message speaking to actual visitors of the defaced page, the style and content needs to change from scene-typical to more general appeal. Finally, the footer speaks to both audiences simultaneously by reminding them once again of the defacement author and offering further reading links.

[45] The HTML sample to produce the “GForce” logo at the very top shows an abuse of the block quote tag, while the rest of the defacement is done in basic but mostly valid HTML. Instead of using the text-align tag, the indentation is realized by combination of nine <blockquote> tags:

```
<blockquote>
  <blockquote>
    <blockquote>
      <blockquote>
        <blockquote>
          <blockquote>
            <blockquote>
              <blockquote>
                <blockquote>
                  <p><font size="4" color="#00FF00" face="Arial,
Helvetica, sans-serif"><i>GFO<font
color="#FFFFFF">RCE</font></i></font><font
color="#FFFFFF"><i><font size="4">
                    </font></i></font></p>
                </blockquote>
              </blockquote>
            </blockquote>
          </blockquote>
        </blockquote>
      </blockquote>
    </blockquote>
  </blockquote>
</blockquote>
```

No images are used and the formatting of the text is done through inline CSS, meaning no external style sheet is used. This might be a strategy to increase the lifespan of this defacement and leave fewer traces, as images and CSS files hosted on 3rd party servers are subject to link rot and not usually captured by archiving bots.

5.5.3 Style

The author takes on the identity of the group when addressing the reader. Even though the individual members of GForce enjoyed a bit of publicity as seen in the interviews, here it was decided the group should speak as a whole. This leads to the strangely hesitant phrase “I think we have given a lot of info...”. However much of the style might be owed to the author’s proficiency of English, some decision was made to use this form of group identity.

5.5.4 Content

The content on this defacement is exemplary of many defacements related to public perception regarding Kashmir yet is contradictory. There are obvious grammar and spelling issues, such as “as I type this from the confront (sic) of my home...”, but the defining aspect is the communicative function of this defacement. The text appears, despite the author’s struggle with the English language, to be an argumentative piece. It is, however, interjected with personalizing statements such as the two mentioned above, contrasting this function. It follows a structure of introduction, argument and call to action. Its argument is the information given in the defacement plus the links. The headings “Reasons for Defacement”, “Its high time to sort this issue out for the following reasons” and finally “Our Demands?” are supposed to structure the content accordingly. The content is contradictory in the sense that it varies between attempting to be the factual report of a neutral observer and an openly anti-Indian position. The sentence structure reflects this on all levels, such as when longer, more carefully formulated sentences are injected with one-word rhetorical questions (“Is this what 21st century is?” Rape? Murder?”) The content speaks for a high level of engagement with the issue – starting with the first sentence declaring the Kashmir conflict to be the most important human rights issue in world history – together with a high level of estrangement from its target audience. As noted, the original site seems to be part of a US-American military education and training facility yet the text lacks any relation to that. Referring back to the section on sentimental writing, the text missed the opportunity to refer to a topic positively associated by the target audience (for example, the War of Independence), but instead refers to the controversial Clinton-Lewinsky scandal.

The reason for this split between aim and effect, between what the text would like to be and what it represents, lies at a deeper level. This defacement, and in fact most similar defacements, are the expression of a dilemma faced by their authors. To explain this, it is necessary to go back to the slogan “Unrestricted

Information", featured on Zone-H. What is implied by "Unrestricted Information" is, in short, the belief that an objective truth exists and that it holds an intrinsic quality making it recognizable. The speaker sees himself/herself as participating in a rationalized debate amongst other, equally informed participants. In such an environment, the audience is assumed to be both susceptible to and cognizant of the better argument:

> critical debate lays claim to being in accord with reason; intrinsic to the idea of a public opinion born of the power of the better argument was the claim to that morally pretentious rationality that strove to discover what was at once just and right (Habermas 1989, 54)

It has been described in previous chapters how such belief is incompatible with the competitive hacking situation facilitated by cybercrime archives. But even more, what the authors experience is a substantial disenchantment. GForce as a defacement group does not see the material conditions through which they themselves and the digital environment they like to engage with came to be. While the limitations of the liberal hacker ethos are unclear to them, they attempt to participate in what they think to be the public sphere, when the greatest significance of their communication is restricted to their own scene. Speaking from a position of "audience-oriented privacy" (Habermas 1989, 51) – that is the often expressed private outrage combined with public political demand – GForce attempts to participate in a public they assume to be governed by an intrinsic truth and rationality. They do not possess any of the required capital – material or cultural – to engage effectively in this bourgeois public sphere model (Calhoun 2010, 23), but nevertheless launch their attempt. Occasionally, they might answer failure by holding the public sphere to its proclaimed bourgeois ideal of free speech and rationality, but overall they fail to be more than an argument unsupported by any capital.

In other words, GForce works on putting information into the network, in the hope of creating a certain effect. When that effect does not happen, or is much less than expected, frustration mounts and eventually turns to anger. This sentiment is palpable all throughout the IRC interview:

> We are doing this to raise public awareness about the Kashmir issue, and how the Kashmiri Muslims (men, women and children), are, at this very moment, being brutally killed by Indian soldiers and no one in the world is doing anything to stop them.
>
> Secondly, we are doing this to show the world how the Palestinian people have been killed by Israeli police, and still are being killed, yet the western media shows pictures of only a few kids throwing stones [...] Once again, no one is doing anything about this, and everyone is just sitting back and watching. (GForce Pakistan n.d.)

This answer hints at what these defacements truly are: the results of a clash between cyberculture and real-world politics, Internet exceptionalism and communication power, an attempt to manipulate public debate and the realization of the contingency of practices to manipulate public debate. Confusing publicity and public, defacers repeatedly attempt to publish information in the hope of engaging their involuntary audience. This strategy might be the reason why defacements over time turn to more evocative and affective material such as pictures and names of victims. It might also be the reason that defacements generally become shorter over time, with multiple paragraphs of text as seen in DefacementId 8986 becoming the exception. As much as the argumentative approach is typical for defacements of the early 2000s, this approach is quickly changed towards a more visual, shorter appeal to readers emotions. Compared to a defacement such as DefacementId 29469446, referencing Gaza in 2014, this older GForce defacement is almost entirely text-based while the more recent defacement relies on pictures and an embedded YouTube video. This development is indicative of changing technological possibilities and skills – YouTube was only launched in 2005 and embedded video was not a web design element on the early 2000s – yet it also shows how the rational-argumentative approach was gradually abandoned in favour of an affective or even sentimental approach.

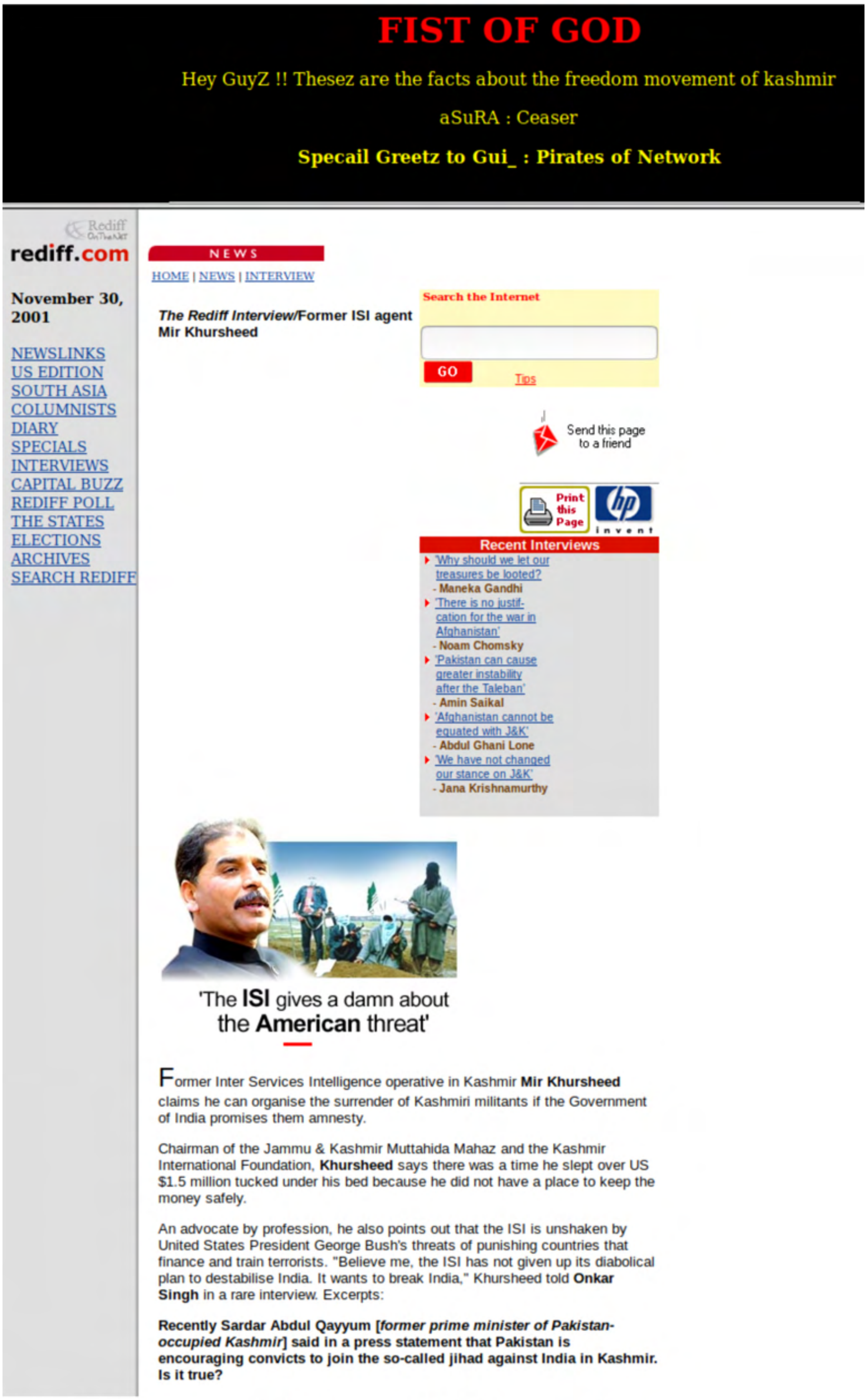
An inherent weakness in the argumentative approach is the referred material. If, in a true Habermasian sense, the defacer assumes rationality to guide debate within the public sphere, and sees his/her own arguments as justified, what may explain inaction? There are two principally different pathways to choose here. The first is to assume that inaction is rooted in disinformation. The defacer's answer then is to publish more, ideally previously unknown material on the same topic in an attempt to either reach a critical mass (defacer assuming a public sphere based on vox populi*)* or to finally make the one argument which gains traction, catches public interest and leads to political action. This first pathway is easy to integrate into feelings of exceptionalism amongst hackers such as the knowledgeable underdog trope mentioned in earlier chapters.

The second pathway is to assume inaction is rooted in misinformation. Here, a defacer assumes established forms of knowledge generation are corrupted and thus public opinion has been manipulated. The defacer's appeal to the public then is lament for the ideals of a rationalized public debate, a common strategy for those who lack the capital to participate in the bourgeois public sphere (cf. Calhoun 2010, 21). The second part – attacking established forms of knowledge generation – is an aspect rarely seen in the analysed defacements. Occasionally that takes on the form of exposing euphemisms and speech regulations such as the term insurgents contrasted with images of dead civilians, but this approach then is not followed through to the extent that GForce would advocate a public independent of established media, based on new forms of communication sealed off from the corrupted mainstream. Looking back at the interviews and information available on the two largest groups in this thematic collection of defacements, GForce and AIC, there is no reason to assume that a disdain for traditional media would be part of any of the two group's image, certainly not for the members of GForce.

In all the disenchantment and frustration palpable in these texts, there is also evident a search for communicative strategies to overcome the dilemma of being able to speak freely but not being able to effectively communicate the message. The defacer does not see the historic conditions which brought about this special breed of techno-utopian liberalism which in turn enabled a hacker identity to be formulated in the first place. What remains for the defacer in the light of this realization is to either move on to other forms of digital activism such as digital culture jamming or cyberwarfare, either way abandoning the idea of effective participation in the public sphere. An alternative to moving on – which prerequires a crisis of the self – is to move inwards, to become a mutually-assuring community of like-minded individuals, at the same time naturalizing one's own perspective and justifying each other's actions. In this respect, the framing of the text with the logo at the start and the greetings at the end can also be read as part of a reaction to this experience of frustration – it is a way of turning towards the kind of public that would value the defacement if not for its political content, for its existence. The following example is well suited to exemplify the search for new and better forms of expression in defacements.

5.6 8190, an outlier

DefacementId 8190 is unique in the sense that it is the only defacement in the Kashmir collection speaking from an Indian perspective. The authoring group, Fist of God, is featured on Zone-H with a small number of not-in-scope defacements but is otherwise unknown. The defacement is an outlier not only in terms of content, but even more so in its structure. In the following it will be explained how Fist of God follows a new approach to overcome some of the limitations described earlier.



FIST OF GOD

Hey GuyZ !! Thesez are the facts about the freedom movement of kashmir

aSuRA : Ceaser

Specail Greetz to Gui_ : Pirates of Network

rediff.com

November 30, 2001

NEWSLINKS
US EDITION
SOUTH ASIA
COLUMNISTS
DIARY
SPECIALS
INTERVIEWS
CAPITAL BUZZ
REDIFF POLL
THE STATES
ELECTIONS
ARCHIVES
SEARCH REDIFF

NEWS

HOME | NEWS | INTERVIEW

***The Rediff Interview*/Former ISI agent Mir Khursheed**

Search the Internet

GO Tips

Send this page to a friend

Print this Page

Recent Interviews

- 'Why should we let our treasures be looted?' - **Maneka Gandhi**
- 'There is no justification for the war in Afghanistan' - **Noam Chomsky**
- 'Pakistan can cause greater instability after the Taleban' - **Amin Saikal**
- 'Afghanistan cannot be equated with J&K' - **Abdul Ghani Lone**
- 'We have not changed our stance on J&K' - **Jana Krishnamurthy**

'The **ISI** gives a damn about the **American** threat'

Former Inter Services Intelligence operative in Kashmir **Mir Khursheed** claims he can organise the surrender of Kashmiri militants if the Government of India promises them amnesty.

Chairman of the Jammu & Kashmir Muttahida Mahaz and the Kashmir International Foundation, **Khursheed** says there was a time he slept over US $1.5 million tucked under his bed because he did not have a place to keep the money safely.

An advocate by profession, he also points out that the ISI is unshaken by United States President George Bush's threats of punishing countries that finance and train terrorists. "Believe me, the ISI has not given up its diabolical plan to destabilise India. It wants to break India," Khursheed told **Onkar Singh** in a rare interview. Excerpts:

Recently Sardar Abdul Qayyum [*former prime minister of Pakistan-occupied Kashmir*] said in a press statement that Pakistan is encouraging convicts to join the so-called jihad against India in Kashmir. Is it true?

Figure 5.10: Screenshot of defacement Id 8190, cropped

5.6.1 Background

The page in question was submitted to alldas.de on the 18th of December 2001 and eventually handed over to Zone-H. The target page was the Chilean site of a subsidiary of PepsiCo.. Text on the target page has been completely replaced by the defacement. There is no recognizable connection between target, audience and message.

5.6.2 Structure

The defacement is divided into two parts. The black top section is the original work of the defacer while the lighter bottom section is an interview with former Pakistani Inter Services Intelligence operative Mir Khursheed published on the Indian site rediff.com on 30th of November 2001. This is created by using two iframe elements, so that the bottom part actually loads the interview from the original site. The top part takes up about half the screen and stands in stark visual contrast to the light layout of the interview. Similar to GForce, this group also features their own name as the most prominent element, followed by a short introductory text (Hey GuyZ !! Thesez are the facts about the freedom movement of kashmir) and concludes with greetings, thus deviating from the aforementioned tripartite design where the content is framed by a header and footer. This defacement does not offer any further reading or contact information, it also does not wrap the message with a footer.

5.6.3 Style

This defacement also features a black background, a design feature very popular with people who preferred to use their CRT monitor in the dark (Lialina 2005). Any text element in the top section stands in contrast to the black background. The text is kept to a minimum and there is no footer with any kind of contact information.

In contrast to this is the light-coloured bottom section. It features the print-oriented layout of an early 2000s news website and is hard to read since the top section of the page stays in place as the user scrolls the page, thus constantly framing the message with its context. This adds a constant reminder to the reader that, even while reading the article, they are still in the context of a defaced site. The omnipresence of the header means that the narrative remains framed by it at all times, increasing its presence and importance. This structure also replaces the need for a footer as the defacer name stays visible, and users do not have to read the text all the way through to be reminded of the defacer's name and intention.

Using an iframe element to divide the page was common practice among amateur web designers in the early 2000s. Through an iframe, an entire page could be used as part of another, without having to duplicate any material, thus saving server space. The use of multiple frames on the same page often leads to usability issues, because scrolling depends on what iframe the mouse pointer is on. This can be seen in the defacement in question, where the bottom section does not scroll unless the mouse is pointed at it. Usability aside, this design is arguably more advanced than the text-based approach described in the previous example.

In terms of longevity, there is a risk in using external material of any kind as it will be subject to link rot. Crawlers might not follow external links, possibly leading to incomplete captures. In this case, it was due to rediff not changing the structure of their site or taking old articles offline that allowed for a complete capture.

5.6.4 Content

The content of this defacement shows how the attacker, with the least possible effort, aimed to achieve maximum effect in attacking the established view of the Kashmir conflict the addressee is supposed to have. By incorporating another source, the defacer circumvents the pitfalls of having to formulate the whole piece in a foreign language for an unknown audience. It further draws upon an established look and layout that viewers are used to. By that it overcomes the sometimes questionable aesthetics popular in early 2000 alternative web design such as the colourful text on black background.

There is speculation on why this piece of information was chosen. At the time of defacement, the interview with Mir Kursheed had been published for almost three weeks so that it was likely not selected for its novelty. Rather I believe it was deliberately selected as part of an elaborate information strategy.

Firstly, this defacement’s content does away with the role of the neutral observer often seen in other defacements. This one does not claim to simply speak in the name of peace; it very clearly shows its stance and allegiance. The author’s anti-Pakistan, pro-India position is made clear in the header and then confirmed in the text. In doing so, the author is still able to communicate effectively. No time is wasted insulting the audience, the carefully established speaker does not break character through unspecific demands. Most importantly, the author is less vulnerable to criticism accusing them of providing only one-sided information, since the author’s perspective and interests are not hidden by false claims to neutrality. The author in general is much less important in this approach, so that less time has to be spent to first establish its role. The speaker does not attempt to participate in a rationalized public sphere and consequently has no need to either demonstrate his/her social capital or, for the lack of it, appeal to the public sphere’s higher ideals. This defacement does not have an “about us” section because there is no need for one. Its communicative function does not rely on the defacer’s reputation.

This approach shows a much better understanding of the functions of media than the previous defacement. Abandoning the neutral observer role means stepping away from the techno-optimistic idea of objective truth as an intrinsic value identifiable to the observer. It also means abandoning the argumentative type of defacement where information is provided leading up to a call to action. Information here is inserted into public discourse and memory is affected insofar as certain events are re-evaluated by the interviewee. Doubts are inserted about historic events and through that, the structure which brought about the public awareness of these events itself is targeted. This defacement on a content level does work by debating the factuality and truthfulness of this or that event. On a meta level it uses information to create doubts and delegitimize the entire Pakistani narrative of the conflict. It is an effective mode of propaganda absent in GForce, AIC and the majority of other defacers active around the Kashmir conflict.

Secondly, the target audience of this defacement is much less specific than in the previous case. To briefly recapitulate, this is an English-speaking interview with a Pakistani former intelligence operative published originally on an Indian news website, now available through a defacement placed on a Chilean website. The target seems to have been chosen at random, probably with the intention to have the highest number of defaced pages possible, to generate the maximum outreach. It stands in contrast to the target of the first defacement which presents some level of affiliation with the expressed call to action and contains passages directly addressing US readers. This defacement, though, does not make any assumption about its audience. While the choice of target shows little specificity, the choice of topic does make it clear that it is aimed at an audience which has to have at least some level of familiarity with situation in Kashmir at the time. It very smartly uses this interview to connect to both sides in the Kashmir conflict through the choice of interviewee and medium of initial publication as well as an international audience by referring to George W. Bush’s foreign policy regarding Pakistan. While the first defacement offers a specific message to a small audience, this one sends an unspecific message to a broad audience. The contents of the interview may not make sense to every involuntary recipient of this message, yet that is a risk this defacement is taking in the hope of reaching some audience capable of doing the contextualizing work required.

The thesis has previously argued that the strategy of breaking into public discourse with arguments based on already known information is at risk of either ending in a loop of repetitions or in a continuous estrangement from the audience. This estrangement might be a first step in radicalising the speaker, when they see their arguments continuously failing to have an effect. Earlier in this chapter it has also been described how defacements can offer a different solution to this problem by incorporating information not previously part of the public debate. Its immediate effect is to possibly draw readers towards the new material. It is unlikely that users are happy to see their target websites replaced by information they could – in similar form – also access through a newspaper or any other traditional news information source. Using novel information has the potential to draw in users or to keep existing users around for longer. But its real strength does not lie in reporting what traditional news outlets do not (yet) know. On a strategic level, this abandonment of public sphere debate ideals and the way it is disseminated is an attack on the whole system of established news outlets. It is a power game (Fuller 2018) where the speaker attacks an understanding of truthfulness itself, forcing the other side into a defensive engagement with the content presented, while the effect unfolds on a structural level.

While the interview itself had been published for almost three weeks at the time of defacement, in combination with the defacement it became a piece of information well suited for this strategy of using information to delegitimize the general truthfulness of the opposing side. The defacement as a form of political communication seems to be especially well suited to transmit such information as it combines the possibility for more detail than graffiti or a poster, and it contains the element of surprise as it appears to the user without warning. It is in this situation that the communicative strategy of the second defacement works much better. To explain better, it is necessary to consider the effect the defacement itself has on the user. On a technical level, defacements are the products of unauthorized access to a system. Usually they are designed to interrupt the normal flow of visitors on a site. In this function, defacements are deconstructive since they break with the illusion of a smooth user experience and confront users with the fact that any system can be reduced to an arrangement of drives and wires, all of which are vulnerable to outside manipulation. Defacements are detournements of the digital as they deny the expected outcome and reroute the user. Their content must mirror that function, it must deny the expected and send the reader's mind down a different path. This is achieved when unexpected content leads to more questioning of a reader's perception of reality. The act of overwriting one electronic text with another has already led to the questioning of the nature of the digital information processing apparatus surrounding the user. Now the content must carry on that momentum into the realm of the political and eventually into the realm of the more abstract information and memory managing systems surrounding the individual. A situationist detournement does not convince anyone of anything, it leads to questioning the nature of experienced reality. Defacements can operate on the same terms if their authors understand these principles.

If the first defacement was emblematic of defacements submitted around the Kashmir conflict, the second one is an outlier not so much in the sense of its political position, or the use of external material. After all, the use of hyperlinks to refer to external material is very common. What really sets it apart is how advanced it is compared to the rest of the collection. GForce, the authors of the first defacement, have been described as looking for a way out of the dilemma of being able to speak freely, but not being able to achieve effective communication. This second defacement is past that stage. It is an example of how an author has adapted a progressive communication strategy and has utilized the defacement as part of that strategy.

5.7 Conclusion

The Kashmir conflict is an emblematic case of real-world events fuelling web defacements of various nature. A cluster of defacements exists around the events which occurred during the long and still unresolved conflict. Amongst the defacements, two groups were most active and featured the most prominent public profile making use of more traditional media forms such as interviews. Through these interviews, both of the most prominent groups, GForce Pakistan and AIC, explain their political agenda and communicative strategy of using web defacements as a tool to increase global awareness.

To achieve their goal of intervention through the creation of public awareness, most defacers active in this cluster employ a strategy of information provision whereby they assume public apathy to be rooted in a lack of public debate caused by a lack of information. Consequently, they aim to provide as much information as possible into an assumed rational public sphere which would in turn recognize them as valid and important. In doing so, defacers usually emphasize their alleged neutrality. This strategy is limited in its effect by the nature of defaced web pages as a medium for political debate, which is described by a short lifespan, varying quality of content and unspecific audience. Increasingly, defacers then output more information or might eventually become estranged from their original audience and possibly turn to more scene-inward communication or more transgressive forms of political participation.

Also in this cluster are defacements attempting to overcome the limitations described above. One is a type listing names of victims. This type can be seen as a precursor to the more empathetic memorial type late seen in the context of 9/11. In shifting the focus from information provision to affective appeal, defacers switch their target from an assumed rational public sphere to an empathetic audience. Another approach is described in the second example of this section. In providing information aimed at destabilizing a narrative frame around reporting on the Kashmir conflict, the idea of participating in a public debate is temporarily laid aside and the medium of web defacements is utilized more effectively in the sense that its random appearance and detouring nature are aligned with its message.

In its conflict, contradictions and struggle for expression between interviews and defaced pages, the Kashmir cluster highlights many of the characteristics typical for web defacements of the time. The following section will show a collapse of the attention economy defacers were relying on so far and how this forced a re-invention of how speaker, audience and message were constructed.

6. Case Study 2 – 9/11

6.1 Introduction

The terrorist attacks of 9/11 had such a profound impact on defacements that it forced defacers to rethink their identity, their message and their audience. In its immediate effect it created a space where the usual tactics as described in the Kashmir cluster no longer worked. While the Kashmir cluster featured some defacements as emblematic and other as outliers, the whole complex of 9/11-themed defacements is comprised of outliers in the sense that new communicative strategies had to be found. Thus, the complex of 9/11-themed defacements as a whole stands out from the usual habitus of other web defacements in the research data set. This makes the 9/11 cluster of defacements a useful tool to contrast against both pre-conceived ideas about the political allegiance of defacers as well as previously established tropes such as the knowledgable underdog – a hacker's version of the rejected prophet.

This chapter will be shaped by its comparative approach and while it aims to be self-contained, it cannot do without explicit and implicit references to the Kashmir cluster as emblematic of typical hacktivist defacements and the previous work on defacer ideology. Where that is the case, explanation and references are given to help contextualization.

The first part of this chapter serves to provide an overview of the available material. It gives an introduction to the defacers and the targets active at this time. Where appropriate, the data will be compared against data from the Kashmir cluster. The overview will also show how 9/11-themed defacements develop slowly in September 2001 and only peaked in October and November. With the differences in data described, the analysis will move on to explain their origins.

An investigation into the most active defacer group in this cluster will bring to light some of their tactics and motivations, while a special focus will be placed on the use of national symbols and declaration of allegiance to a nation/al cause. This is necessary to understand how a range of solidarity, grief, nationalism, and anti-terrorism statements are found in the 9/11 cluster which is surprising considering the disdain defacers show for anything mainstream.[46]

To look more closely at how 9/11 led to new ideas of how defacers present themselves, what and to whom they communicate, three general categories of

[46] Emblematic for this disdain is the Hacker Manifesto's description of the society in which the speaker grew up:

> You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.
> (The Mentor 1986)

defacements are identified and described. These categories generally represent different phases in reaction to the events of September 11, 2001 and are classed as memorial pages, reactions to the Patriot Act and – following years later – passing references to 9/11.

The conclusion will bring together the findings of all different sections of this chapter and positions them within the theoretical framework of an attention economy. In reference to the previous case study, the question of whether defacers aim to reach an outside audience or are mostly communicating amongst themselves will be dealt with, while acknowledging the unprecedented circumstances 9/11 had put defacers in.

6.2 Overview

This section serves as an introduction to the defacer groups active within the 9/11 cluster as well as the temporal and spatial (domain-specific) distribution of defacements. Since one defacement group was active in the 9/11 and the Kashmir cluster, their attack profiles are compared.

6.3 Notifiers

There are a total of 35 web defacements identified as directly relating to 9/11. 10 different groups or individuals submitted defacements to the Zone-H archive, with 4 groups or individuals submitting more than one defacement. The top two groups account for approximately 60% of all submissions. This is similar to the distribution in the Kashmir cluster where the majority of defacements was submitted by a small number of very active groups. The most active group, BHS, will be discussed in more detail. Interesting to note is that the second most active group AIC is also one of the two most active notifiers in the Kashmir cluster.

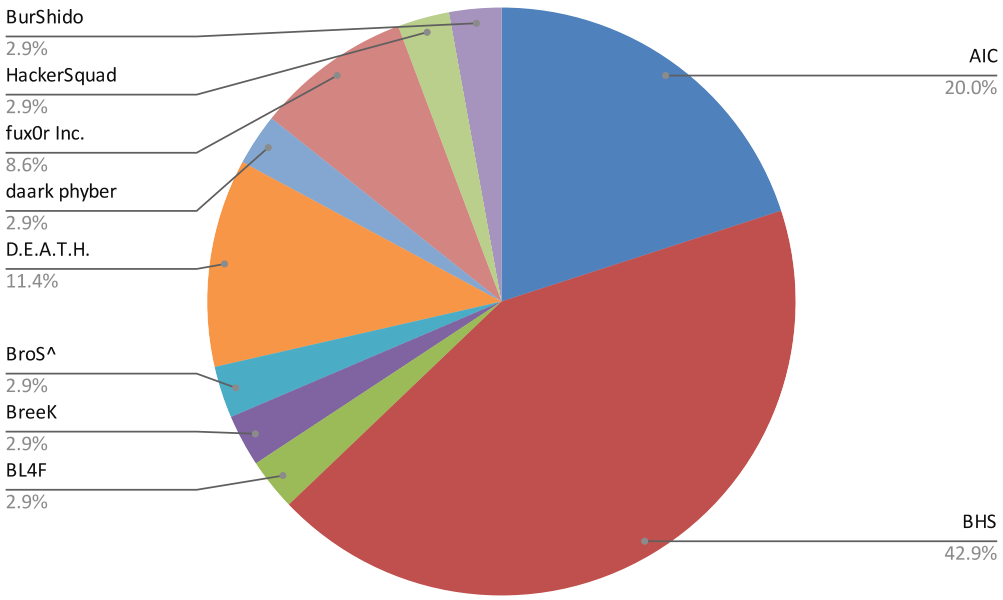
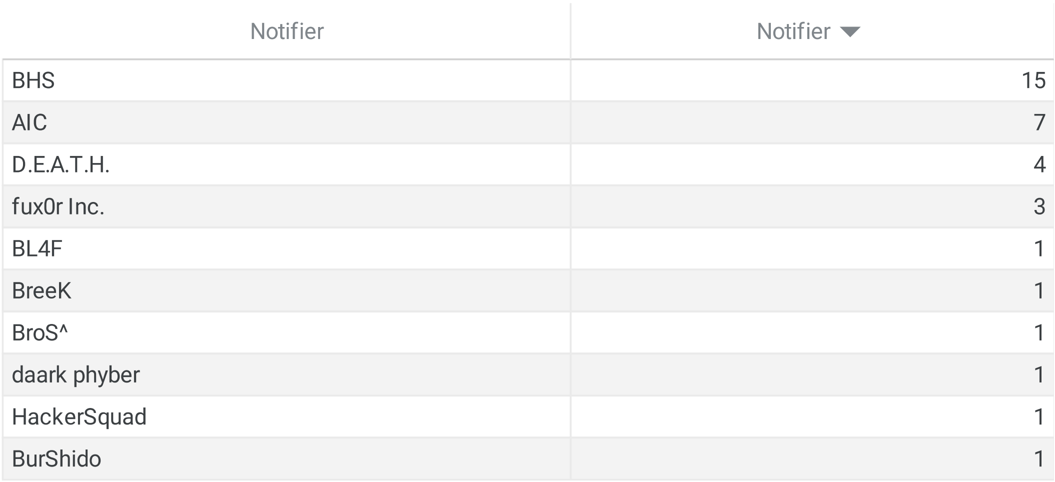


Figure 6.1: Distribution of defaced pages by group as % of total



Notifier	Notifier ▼
BHS	15
AIC	7
D.E.A.T.H.	4
fux0r Inc.	3
BL4F	1
BreeK	1
BroS^	1
daark phyber	1
HackerSquad	1
BurShido	1

Table 6.1: Distribution of defaced pages by group

None of the defacers in the above list are exclusively focussed on 9/11; all have submitted various other defacements before or after September 2001. The defacer most focussed on 9/11 and terrorism is a collective called Defenders Evaporating And Terminating Hate, or D.E.A.T.H.. The group submitted a total of six defacements[47] with 4 directly referring to 9/11, one featuring a poem written by one of the members of D.E.A.T.H., and the other one featuring the poem *Death of an Innocent*[48], a popular text on the Internet during the early 2000s. This indicates that following 9/11, at least one group of defacers got together to form up under the acronym D.E.A.T.H.. Other groups seem to have preferred to use their existing and established identities, possibly to use and further expand their existing reputation.

Comparing overall numbers, 9/11 did not see as many defacements as the Kashmir Conflict (35 vs 116). The reasons for this are unknown. A possible reason might be the high level of media coverage for 9/11 while many of the topics usually covered by web defacements see little public attention in established media. Engaging with a topic so extensively featured in mainstream media made it hard to maintain anti-mainstream positions and an underdog image and thus may have made creating effective defacements more challenging and so reduced the number. It is also entirely possible that defacers did not so much choose the topic of 9/11, but that the changing legal conditions around hacking brought about by the *Patriot Act* that legislated against hacking and which was enacted at this time meant the topic could no longer be avoided. In the following examples, evidence for both will be presented.

6.4 Distribution of targeted domains

It has been described in previous chapters how two general approaches exist for choosing targets for web defacements. A defacer might select targets for ease of access, with the intention to deface as many pages as possible within a short time, or an attacker might attempt to make a statement by hacking a page which is difficult to get access to. The existence of both strategies is confirmed by Romagna and van den Hout (2017, 7) while automated defacement programmes scanning the web for pages with known vulnerabilities and automatically defacing them are described as a popular way to increase outreach capacity by Maggi et al. (2018, 445–46). In this regard, the distribution of TLDs as targets in the 9/11 data subset reflects both strategies.

[47] See http://www.zone-h.org/archive/notifier=D.E.A.T.H.

[48] See https://www.poemhunter.com/poem/death-of-an-innocent-6/

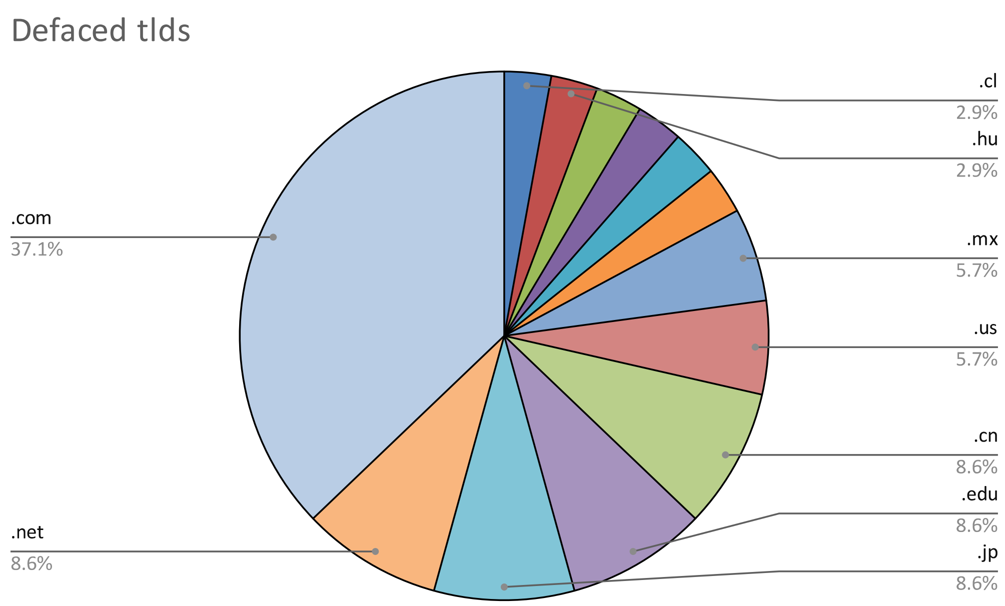
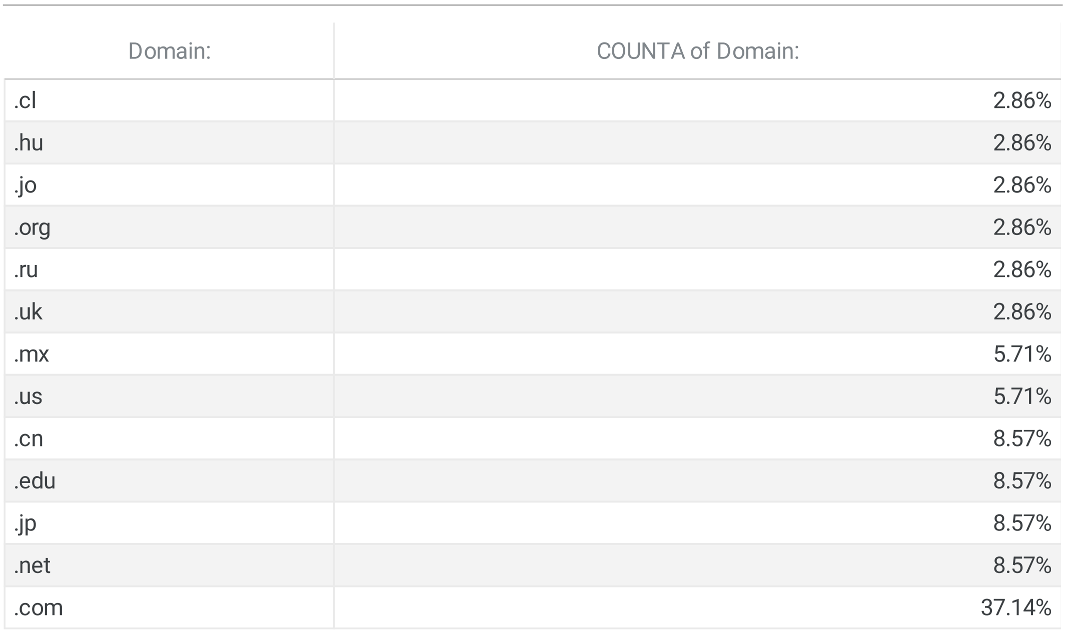


Figure 6.2: Number of TLDs defaced as % of total



Domain:	COUNTA of Domain:
.cl	2.86%
.hu	2.86%
.jo	2.86%
.org	2.86%
.ru	2.86%
.uk	2.86%
.mx	5.71%
.us	5.71%
.cn	8.57%
.edu	8.57%
.jp	8.57%
.net	8.57%
.com	37.14%

Table 6.2: Distribution of defaced TLDs

As was the case in the Kashmir cluster, .com domains make up the majority of defaced domains, followed by .net domains. These generic domains are followed by country-specific domains (.jp, .cn, .us, .mx). In comparison to the distribution of TLDs in the Kashmir cluster, where .com alone made up 57.89% of all defaced TLDs, the distribution of targets around 9/11 shows much fewer generic TLDs and significantly more country-specific domains. Since both sets of defacements cover approximately the same time period, it is deduced that these different results are due to different strategies of communication where country- or audience-specific TLDs are targeted to better reach a defined audience. In support of this finding is the very interesting crossover of AIC, the second-most active defacer in both clusters. While in defacements submitted in the Kashmir cluster, AIC had a focus on .com and .net domains, in defacements submitted in the context of 9/11 the focus shifted to .edu and .us domains. The case of AIC being active in both clusters gives the opportunity to compare different target selection strategies in defacements. The following visualization compares the TLD profile for AIC in both clusters:

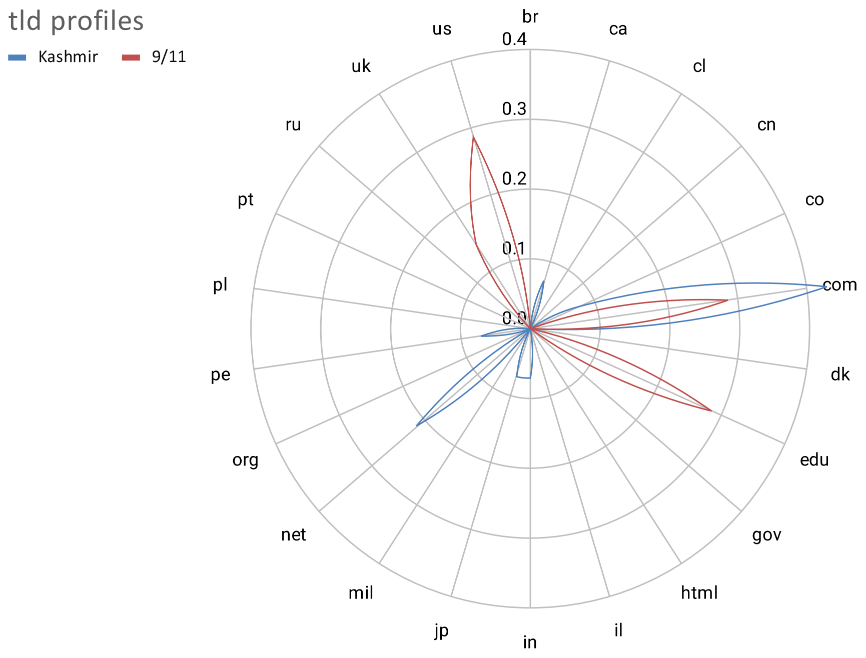


Figure 6.3: TLD profiles for AIC compared

This comparison enables us to see how country-specific TLDs such as .us and .uk are not targeted at all in the Kashmir cluster, but are central in the 9/11 cluster. Further, .net domains are not used at all in the 9/11 cluster while .edu pages become a target. The fact that the distribution of attacked TLDs clearly diverges from the overall distribution of TLDs shows that a deliberate strategy was used to define targets.[49] Comparing the two profiles then shows a decline in the use of .com domains as targets during the 9/11 cluster and a strong increase in domains serving an English-speaking, western audience (.us, .uk, .edu). This suggests that the point of defacements around 9/11 was to reach an Anglophone audience. As the following analysis will show in more detail, this Anglophone

[49] It was not possible to obtain reliable figures for the distribution of TLDs in 2001. 2008 figures show .com being the second-most numerous TLD after .net. The top 5 are thus .net, .com, .jp, .de and .br (ISC 2008).

audience was indeed perceived as a rational public sphere with Western sensibility and not as a military of ideological enemy. The 9/11 profile shows an increased attempt to communicate with a western audience and provides evidence that targets have been selected according to this effort. The comparison of AIC's target profile shows that AIC strategically picked targets for each campaign. These are both indicative of a high level of planning and a strategic aim in their defacement campaigns.

In the context of defacements around the Kashmir conflict, defacers have spoken of a net war between India and Pakistan, with their defacements being a subversion of the enemy's digital infrastructure. In the case of the 9/11 defacements, there are no obvious targets to be found for defacers sympathetic to the US cause. The conditions of asymmetric warfare extend into the virtual insofar as Al-Qaeda does not have a web presence to attack. The extensive use of online media in terrorism was only established years later by the Islamic State.[50] For the immediate post-9/11 period covered by the defacements in this cluster, defacers speak sympathetically to a western audience. In mourning and remembering the events, defacers demonstrate alignment with the public reaction and at the same time claim their place as part of that public.

Shared emotional states, sympathy and sentiment are fundamental to democratic societies (Douglas 1988; Barnes 1997; Burstein 1999). While appeals to these are also used in the Kashmir cluster to engage foreign audiences and bridge cultural and linguistic barriers, emotional states are central to 9/11 defacements where defacers want to participate in these appeals rather than create them. In an overview, the 9/11 defacements are more reactionary than the Kashmir defacements in that they offer much less new information and – as confirmed by the AIC attack profile comparison – they attempt to engage an audience whose approval they seek.

[50] For more detail on the use of media in Islamic terrorism, see Atwan (2015).

6.5 Temporal distribution of attacks

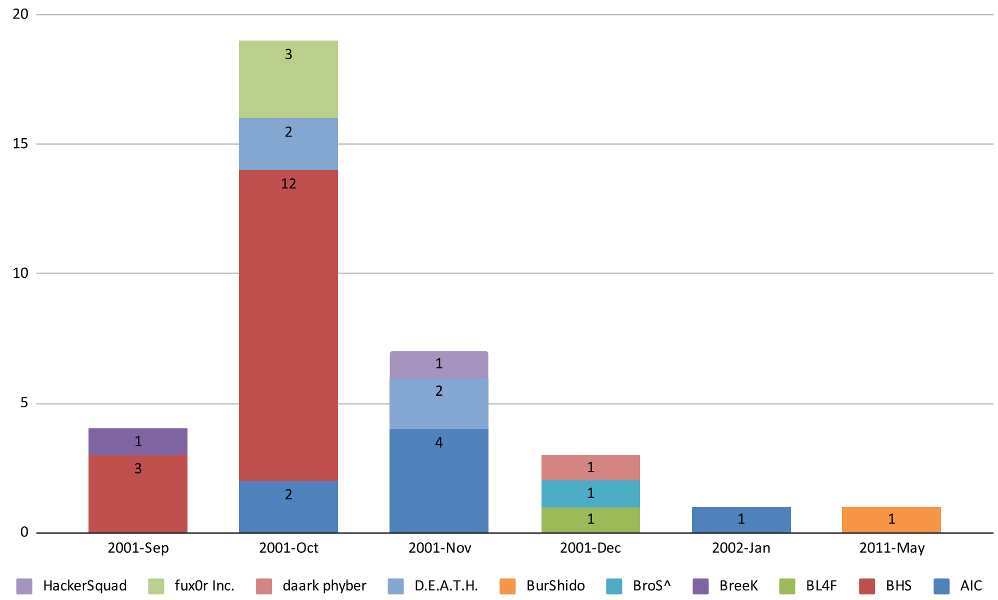


Figure 6.4: Defacements by month and notifier

The temporal distribution of attacks must be read with the limitations of the methodology of this study in mind; while as many pre-2000 defacements as possible were collected, only 2000 more recent defacements were collected in order to produce a manageable, but still arguably representative data set. Still this randomized approach yielded a 2011 defacement referring to 9/11, however the focus of the cluster is the time period from September to December 2001.

What is noticeable at first glance is the delay between the September 11th attacks and submitted defacements. With only four defacements submitted in September, October 2001 is by far the month with the most defacements followed by November 2001. The reason for this is unclear. While a defacer could hold on to a defaced page and only submit it to Zone-H at a later point, this seems unlikely as it presents no benefit to the attacker. Other researchers have described the timestamps' trustworthiness as “Medium-high”, explaining that “The attacker will get poor visibility by forging this datum” (Maggi et al. 2018, 445). This assessment is in line with my own observations. The observed delay is indicative of the 9/11 defacements being anything but spur-of-the-moment reactions to an ongoing event. As aforementioned in the analysis of targeted domains, defacers show a high degree of planning and coordination between groups (Maggi et al. 2018, 446). Any delay then is best explained by the fact that it took at least three weeks for most campaigns to gain traction and produce defacements which would be archived by Zone-H. The 9/11 cluster thus gives good insight into the planning and execution phase of a defacement campaign by providing a clear reference point for the event they discuss.

Another observation to make is the varying activity between defacers. The most active group, BHS, started submitting defacements as early as September 2001, peaked in October 2001 and then did not submit any 9/11 related defacements again. The second-most active defacer group, AIC, did not submit any defacements until October 2001, had its peak activity in November the same year and then submitted another defaced page in January 2002. These different activity profiles show the different priority the subject had with different groups. It shows that the defacer groups with a high level of coordination such as BHS and AIC engaged with the subject as early as September 2001 and had largely ended their engagement by November of the same year. As BHS represents the most active defacer in this cluster, the group will be analysed in more detail in the next section.

6.6 Nationalism and Allegiance in the Case of Brazil Hackers Sabotage (BHS)

The most active group in the 9/11 cluster is Brazil Hackers Sabotage (BHS). BHS consists of three members with the alias JShalom, Astek and TuK. This group did not only submit the most defacements in reaction to 9/11 they were also featured in a 2002 interview describing their motivation to engage in defacements. What makes BHS worthwhile as an object of study in the context of this chapter is their strong reference to national symbols and their claim to allegiance with Brazil. BHS thus presents an excellent starting point to understand the use of national symbols, nationalism, and claims to allegiance with a national cause used in defacements.

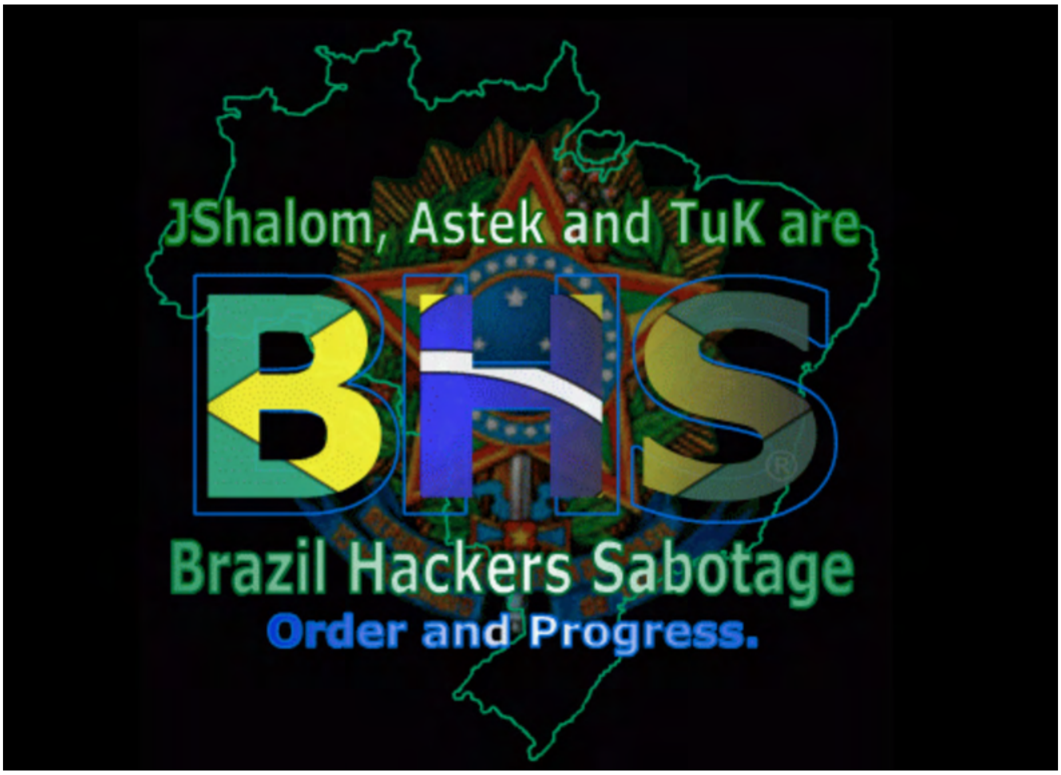


Figure 6.5: BHS logo showing member names.

The logo of the group (Figure 6.5 above) shows the outline of the state of Brazil together with the Brazilian coat of arms. The slogan “Order and Progress” is a translation of the Brazilian state motto “Ordem E Progresso”. There are a number of noteworthy aspects about this logo which give insight into the self-understanding of BHS.

Firstly, the logo is entirely in English, even though the group in its name and insignia shows strong reference to Brazil. This is indicative of BHS’ desire to communicate with an English-speaking audience while remaining recognizable as a Brazilian group. Consequently, BHS defacements are in English and avoid topics that would be of solely Brazilian interest.

Secondly is the striking association of BHS with the Brazilian state. The above logo shows not one, but four references to the nation of Brazil: the country’s outline, coat of arms, national motto and flag. This goes as far as placing the motto “order and progress” right under the words “hackers” and “sabotage”. It remains unclear what BHS attempts to achieve for the Brazilian national cause by defacing web pages, however the logo suggests a high level of alignment with the state, almost to the point where BHS appears to be a state-sponsored group (which it is not).

There exists a second version of the BHS logo, also used in the 9/11 cluster of defacements.

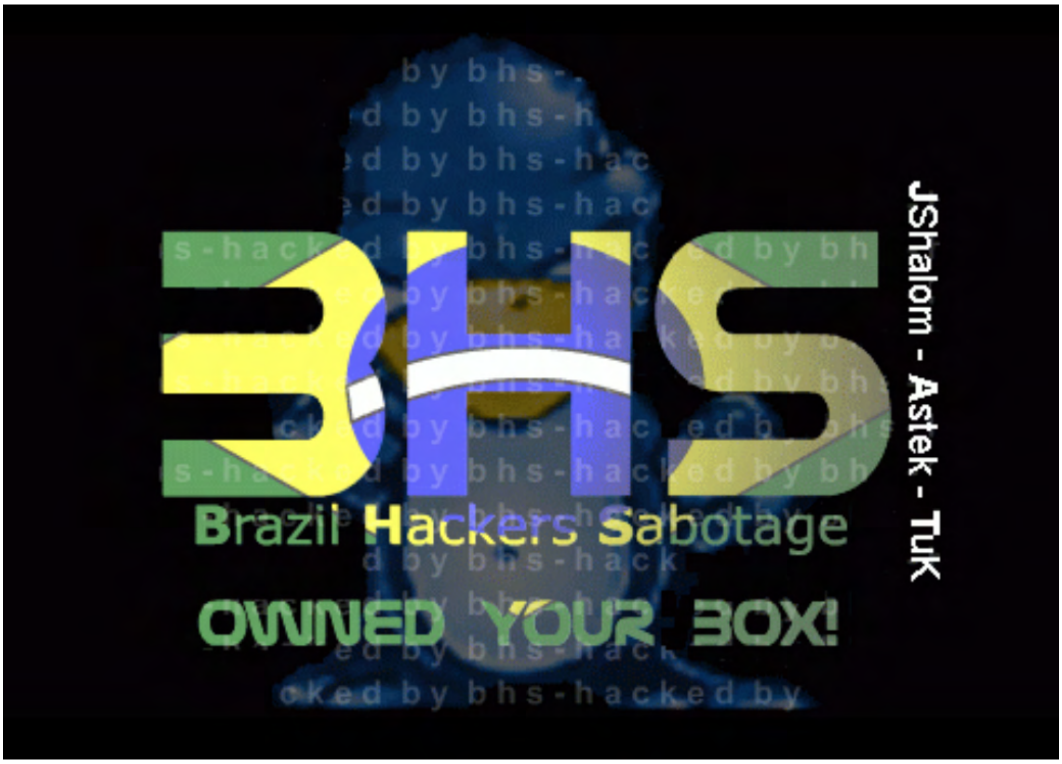


Figure 6.6: Second version of the BHS logo

This version retains some of the features of the first logo, such as naming the members of BHS, explaining the acronym and being written in English. A reference to the Brazilian flag is also to be found, however the rest of the national insignia has been removed from this second version. The country outline has been replaced by a variation of Tux, the Linux brand character ('Linux Logos and Mascots' n.d.).

With the change in design also came a change in addressee, while the first logo communicates a nonspecific message about the members of BHS to any visitor of the defaced site, this second version addresses the admin of the defaced site to send the message that BHS broke the site's security. With this in mind, the first version of the logo must be seen as a self-description while the second version is an attribution or declaration of authorship and skill. The reason for the change is unknown, but since both logos are quite different in style and message, it can be assumed that they were created by different members of BHS and reflect the different motivations within the group. In an interview with the Quebec magazine *Zataz*, a member of BHS called SilentStorm explains the group's motivation and affiliation with Brazil.

The interview consists of 14 questions and was initially published in French, with an English translation added later. Although the translation is crude, no essential information has been lost in the process and thus the English version will be used throughout.[51] The interviewee's alias is SilentStorm, a name not featured in the two logos discussed earlier. Defacements post-2002 however list SilentStorm as a

[51] See the original French version https://web.archive.org/web/20021201122849/http://www.zataz.com/zatazv7/bhs.htm

BHS member, replacing Astek.[52] Whether this is just a name change or Astek left the group and was replaced by a new member is not clear. Indicative of the latter is the fact that defacements by BHS submitted after the alleged replacement of Astek show none of the Brazilian nationalist symbolism found in the earlier defacements but rather focus on attributing the hack to the superior skills of BHS. In the light of this change, the statements given by SilentStorm can be seen as not only the current situation of the group in 2002, but also as indicative of the change BHS had undergone. The group is introduced by the interviewee as:

> The "Brazil Hackers Sabotage" (BHS) is a group founded on March 2001, and it is formed by three brazilians (JShalom, SilentStorm and TuK). The main focus is 'defacements' and the study of technics and codes to create new attack methods. […] The group objective, since its foundation, is to win the challenge of being the greatest 'defacer' group of the world. (SilentStorm 2002)

With its objective of topping the leader board, BHS submitted a total of 1227 defacements to the Zone-H archive between 2001 and 2005. An impressive number, yet a far cry from the 12906 defacements needed to even appear on the current leader board of the most active defacers on Zone-H.[53] The interviewee describes BHS’s focus as divided between web defacements and the creation of new attacks. It is important to note here that BHS does not describe any substantive political agenda. Rather all aims mentioned are internal to their defacement subculture and their subcultural capital. Former member Astek is not acknowledged in this passage or anywhere throughout the interview. Further, SilentStorm does not make any reference to Brazil or the use of state insignia here. The interviewer does not follow up on Astek or the obvious change in corporate design BHS had undergone. Only one question is asked about the Brazilian hacking scene:

> [Interviewer] How many groups of Hackers exist in Brazil ?
>
> [SilentStorm] Brazil has a lot of people involved and interested by web security and attack's. The majority is of young people (from 15 to 25 years old), seeking just knowledge and fun, fact that makes Brazil full of hacker groups. (SilentStorm 2002)

While the interviewer’s question remains unanswered, “knowledge and fun” are named as motivation in hacking. This is in accordance with what previous chapters described as the roots of hacktivism, especially the act of engaging with computer systems as a rewarding activity in itself. SilentStorm reiterates this motivation later on and adds that political or personal motives also play into the defacements:

> The attacks give us two essential things: knowledge and fun. The possibiliy of having them both together is what makes the activity so interesting. […] The essential motivation, like i said before, is the seek of knowledge. Who has more knowledge in this area, is the best. Sometimes we have 'external' motivation, like political or personal things... but just sometimes. Making defacements on government servers, saying what you think about them is very interesting. (ibid)

[52] See http://www.zone-h.org/mirror/id/28522

[53] Counting by total defacements, see http://www.zone-h.org/stats/notifier

The interview as a whole is a mix of uninspired, standard questions and stereotypical answers. Remaining questions cover their fear of prosecution (none), the future of BHS (will continue to hack) and the role of hackers (will always rule the Internet). Unlike AIC and GForce, BHS does not have a website linked in their defacements. While it is unfair to expect SilentStorm to produce a theory of hacking in this context, and the awkward translation from Portuguese to French to English only adds to the interview's casual character, the above passages are worth looking at as they offer some indication of the self-understanding of web defacing groups. The central point is that, for SilentStorm, knowledge is key for participating in defacements. In line with the previous observation of hacking as a meritocracy where the most skilful hacker has the power to overwrite any message, knowledge is heralded as key qualification to participate in a public debate via web defacements. In Habermasian terms, this strategy attempts to bypass the social exclusiveness of the public sphere by substituting (sub)cultural capital in the form of hacking skills for formal education or financial capital (cf. Habermas 1989, 131–32). This is emphasised when SilentStorm explicitly mentions government servers and the rewarding feeling while defacing those. As a logical consequence, BHS has a medium to long-term strategy of investment where they invest time and energy to produce their own knowledge about attack methods to be able to deface more sites.

It is worth dwelling on this point for a while since the idea of defacements as a level playing field where the only capital required is knowledge – and that knowledge is freely available to the enquiring mind – is central for many web defacement groups. This idea links back to the hacker ethic, particularly to hacking as a participatory meritocracy. In applying this perspective, the interview is contextualized in line with the previous chapters describing the theoretical framework of hacktivism while it is also reframed from a banal exchange to a piece of evidence for the described theory. In this point lies the central motivation for groups to even engage in this competitive hacking scene.

The envisioned digital locus amoenus then is twofold; it is a safe space where social divisions do not exist and all resources are obtainable, yet at the same time it is also a space from which the public sphere can be influenced. Hacking is seen as, to use the appropriate lingo here, literally an exploit of society. The practice of hacking is shaped by its genealogy which is outlined in detail in the History of Hacktivism section in Chapter 2. For the context of this section, the apparent conflict between the lack of a distinct political agenda on the side of defacers and the use of defacements for political communication together with legal persecution of defacers can be described as the inherent conflict between smooth and striated space as described by Deleuze and Guattari as:

> two antagonistic operations and interpretations of territory. Smooth spaces are the territory of the nomads, while striated spaces are created by the sedentary – by settled societies developed after the advent of agriculture. Their conflict is a confrontation of movement and speed, arborescence and rhizome, royal science and nomad science. (Ayiter n.d.)

The conflicts between defacers, defaced sites, actual audience and intended audience can thus be described as a problem of translation and transfer between these spaces. Transitioning from the smooth to the striated can be seen when BHS expresses their plan to land IT security jobs through the reputation built as defacers while attempts to regulate and prosecute defacers originate in the striated space. The complexity of translation is stressed by Deleuze and Guattari:

> Translating is not a simple act: it is not enough to substitute the space traversed for the movement; a series of rich and complex operations is necessary [...]. Neither is translating a secondary act. It is an operation that undoubtedly consists in subjugating, overcoding, metricizing smooth space, in neutralizing it, but also in giving it a milieu of propagation, extension, refraction, renewal, and impulse without which it would perhaps die of its own accord … (Deleuze and Guattari 1987, 486)

It is in the light of this theory of space that the following defacements submitted around 9/11 must be seen. They are attempts to speak from a smooth space of playful transgression to a larger public. The reason for defacers to try and communicate with a larger public outside the hacking and defacement scene is the shift public debate underwent post 9/11. With the attention economy in turmoil, defacers had to re-orient themselves. This process will be discussed in detail in the remainder of this chapter, where individually selected defacement emblematically stand in for general trends.

6.7 Defacement types

Relevant defacements around 9/11 can generally be broken up into two main categories. The majority of all defaced pages are memorial sites dedicated to the mourning of the victims, the remembrance of the events and the expression of solidarity with victims. Other defacements are concerned with the immediate consequences of 9/11 and range from anti-terror statements to support of the invasion of Afghanistan, to critical commentary on the Patriot Act. A few defacements only passingly mention 9/11 while developing other, US-centred arguments.[54] While the two categories can be seen as generally different approaches, within each approach exist a range of sub-categories. The following will contrast a range of these sub-categories to arrive at a better understanding of defacers' motivation to partake in 9/11 centred defacements.

6.7.1 Memorial pages

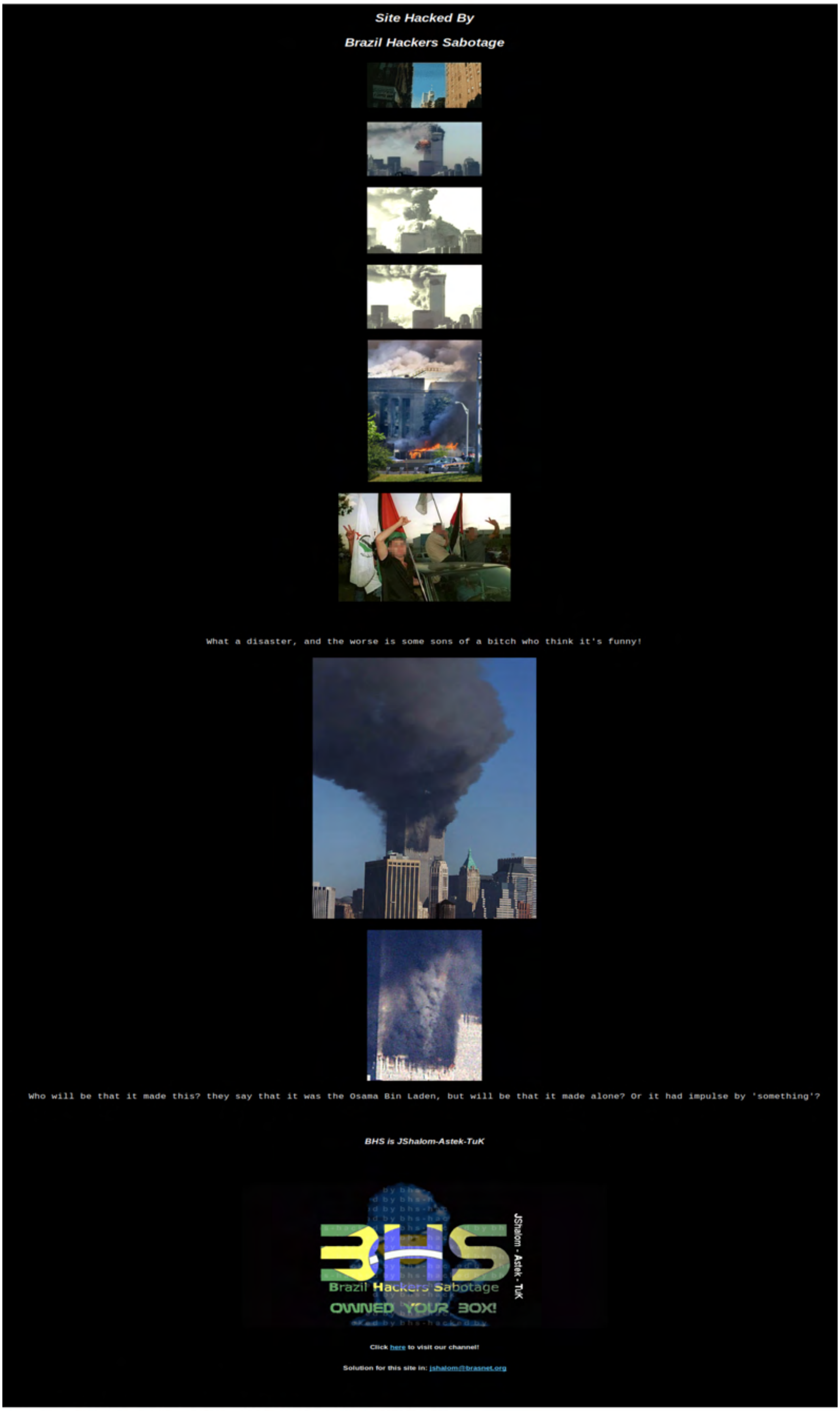
Memorial pages are those primarily dedicated to the memory of 9/11, with few and non-specific political demands within them. Their focus is the mourning of lives lost and the expression of solidarity with the victims. Memorial pages can be reliant on imagery (as will be seen in the BHS defacement, Figure 6.7) or can be text-based. A shared characteristic amongst all memorial pages is their appearance as an initial and sudden reaction to the events as they are happening or have just

[54] An example of this is DefacementId 3249 which starts off relating to 9/11 to then switch to an anti-Semitic conspiracy theory.

happened in the recent past. Looking at the timeline of submission in this cluster, however, it becomes clear that the very first defacement was not submitted until the 26th of September. This delay contradicts the memorial pages' claim to be spontaneous empathetic reactions and reveals them to be artefacts of a planned communication strategy.

9/11 was certainly not an under-reported event. For much of the remainder of 2001 and well into 2002, the event and its consequences dominated international headlines. Remembrance of the dead of course was an integral part of the US government response, and 9/11 also saw excessive coverage in film, series, blogs and original websites (Jarvis 2011; Paganoni 2011). The question thus remains why defacements remembering 9/11 were submitted in the first place, and why it took over two weeks for them to appear. There are no statements in any of the defacements to at least partially answer these questions. Drawing on previous observations of defacer's motivation, my proposed hypothesis is that these defacements are a reaction to the competitive situation of an attention economy. To remain relevant, defacers simply had to engage with popular topics. This is not to say that empathy, genuine shock and possibly the desire to express one's political allegiance played no part at all in the set of memorial pages, yet the long delay suggests those not to have been the only motivators.

The first memorial page to be discussed here is also the first defacement in the 9/11 cluster, submitted on the 26th of September 2001. This defacement by BHS is the first in a series of similar defacements, however this is the only one with a full capture of all images.



Site Hacked By

Brazil Hackers Sabotage

What a disaster, and the worse is some sons of a bitch who think it's funny!

Who will be that it made this? they say that it was the Osama Bin Laden, but will be that it made alone? Or it had impulse by 'something'?

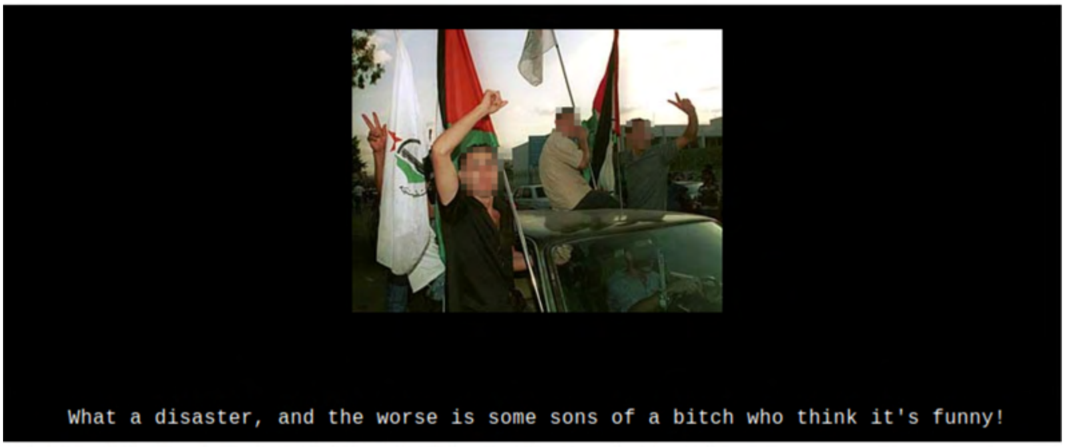
BHS is JShalom-Astek-TuK

Click here to visit our channel!

Solution for this site in: jshalom@brasnet.org

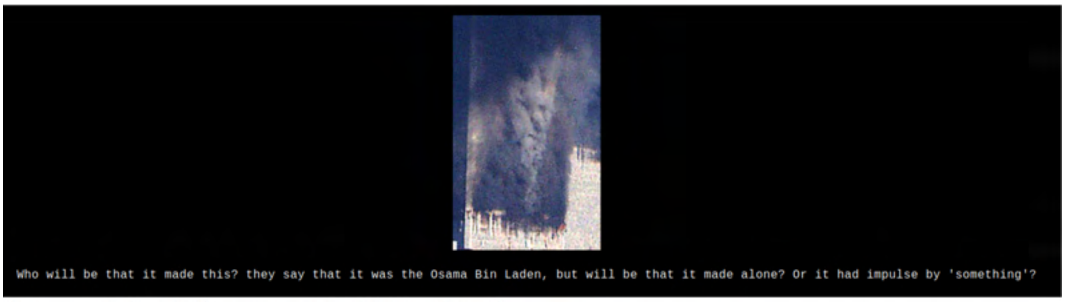
Figure 6.7: DefacementId 2112, full capture

As can be seen, this defacement is image-based. The top two images in this capture are moving images in the original defacement, showing both towers being hit. Structurally this defacement follows the classic structure of header-body-footer, black background and centre-aligned text. There are no greetings or any messages for the defacement community in the footer of this defacement, and the logo has already been changed from the Brazilian insignia to an angry-looking Tux. On a content level, this defacement relies on images to express shock and disapproval for Palestinians apparently celebrating the attacks (Figure 6.8): “What a disaster, and the worse is some sons of a bitch who think it's funny!” BHS also mentions the alleged Devil Face (Figure 6.9) in the last picture, a common theme when after the initial shock observers started to look for explanations.[55]



What a disaster, and the worse is some sons of a bitch who think it's funny!

Figure 6.8: DefacementId 2112, detail. Faces pixelated



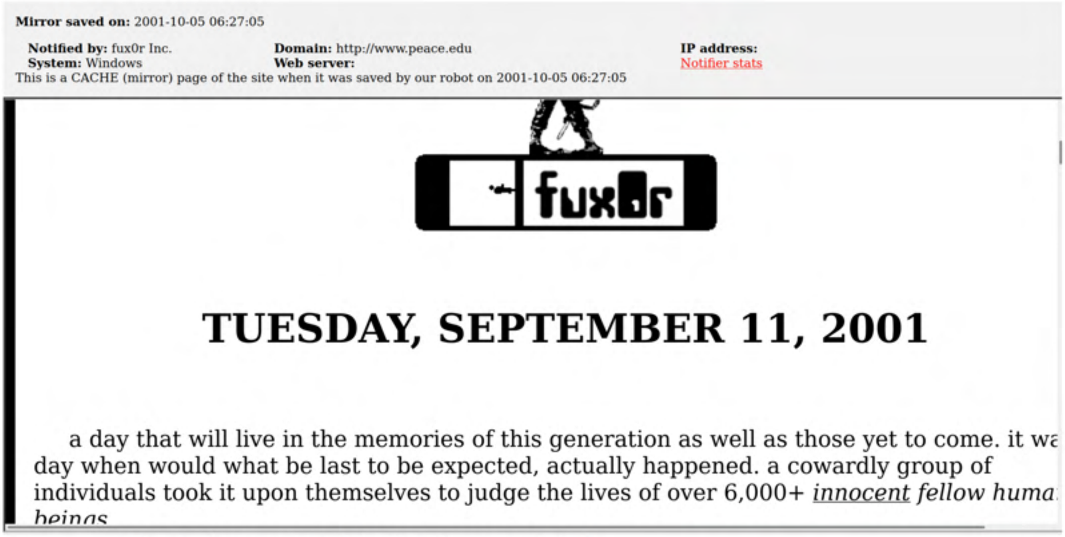
Who will be that it made this? they say that it was the Osama Bin Laden, but will be that it made alone? Or it had impulse by 'something'?

Figure 6.9: DefacementID 2112, detail

This defacement shows the immense shock 9/11 caused even in a Brazilian hacking group. The group must have felt the need to submit a 9/11 defacement even though the event at this stage was 15 days ago. In its reliance on pictures, the lack of explanatory text and the lack of explanation aside from blaming Satan or the Palestinians, the defacement re-enacts the events of September 11th. The first two pictures are snippets of both impacts, filmed at close range while all subsequent pictures remove the viewer more and more from ground zero until the

[55] See https://nymag.com/news/9-11/10th-anniversary/satans-face/

smoke-covered skyline is seen. Scrolling down from the top on a 2001 monitor, this defacement would appear as a slide show transporting the viewer to the streets of New York during 9/11. The shock provided by the content is further emphasized by the shock effect the unexpected confrontation of the viewer with the defaced page exerts. It is in a configuration like this that the defacement as a communicative form works best, mirroring in its disruptive effect on online communication the disruptive effect of its content. The sudden flow of images the viewer is exposed to re-enacts on a smaller scale the global flow of images that has become synonymous with 9/11. This defacement is thus more than a memorial page; it is an attempt to relive the trauma brought about by 9/11 and through repeat exposure to the iconic images, extract some sense from them. In being more than a memorial page, this defacement is both aimed at the unsuspecting visitor as much as it is an attempt for the author to overcome a trauma by re-living it. Responsibility for the attacks is touched upon, but only in a superficial way. There are few calls to action found, other than an expression of solidarity with the victims and a condemnation of any endorsement of the attacks, a topic BHS would develop into a longer argumentative text in later 9/11 themed defacements. As this is the first defacement in the 9/11 cluster, it stands in as an expression of defacements created in the immediate aftermath of the events. It is less concerned with a message but with an effect. This is, however, not true for all memorial defacements as the next example is going to show:



Mirror saved on: 2001-10-05 06:27:05

Notified by: fux0r Inc. **Domain:** http://www.peace.edu **IP address:**
System: Windows **Web server:** Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2001-10-05 06:27:05

TUESDAY, SEPTEMBER 11, 2001

a day that will live in the memories of this generation as well as those yet to come. it wa
day when would what be last to be expected, actually happened. a cowardly group of individuals took it upon themselves to judge the lives of over 6,000+ *innocent fellow huma beings*

Figure 6.10: DefacementId 8525, logo and title

This defacement was submitted by a group called fux0r Inc. on the 5th of October 2001, making it part of a second wave of defacements which are less concerned with the trauma of 9/11 than with a call to action. This defacement is kept in black and white, with a black border resembling an obituary notice in a newspaper. Structurally, this defacement is another example of how widely used the tripartite structure of header-body-footer is. The header introduces the group with not one, but two logos:

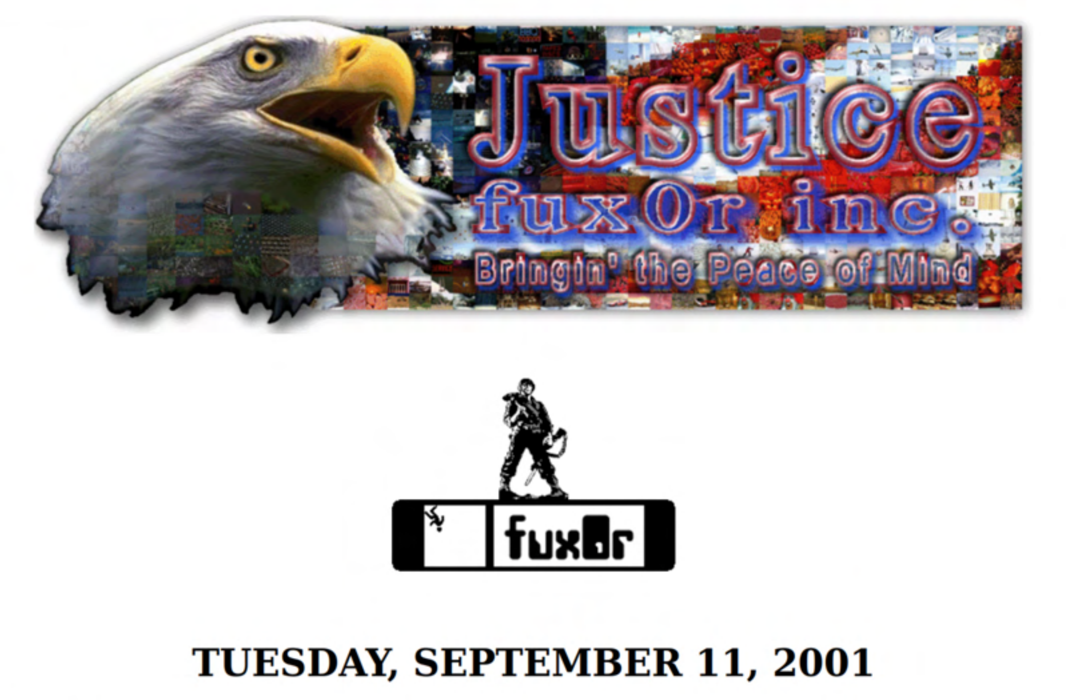


Figure 6.11: DefacementId 8525, full header

While Fux0r Inc. submitted a total of 304 defacements between 2000 and 2002 using a variety of logos, the upper logo seems to have been created in reaction to 9/11 and the lower logo is used on most other defacements.[56] Similar to BHS' logo, national symbols are utilized. The content of this defacement is text-based with a few Associated Press images of the burning World Trade Center featured towards the end. Following on in the established structure, the footer then contains greetings to fellow hackers and, surprisingly, "the dispatchers", probably meaning emergency service personnel coordinating the disaster response that day. It is unlikely to think that many of them, should they ever come across this page, would appreciate the greetings fux0r Inc. sends out here. Rather than being a greeting directed at dispatchers, this line appears to be a virtue signalling practice to help position the defacers as clearly aligned with the cause of the US-American public in October 2001. No other sources such as interviews or homepages are available to provide more information this defacer.

Before looking closer at the content of this defacement, the target selection must be discussed. The defaced page is the online presence of the William Peace University in Raleigh, North Carolina. This clever target selection enables fux0r Inc. to successfully act on two objectives at the same time. Defacing a US-American .edu domain means that the message will be seen by a relevant audience of young US citizens that have all recently experienced 9/11 as a profound and tragic event. The domain itself, peace.edu is of course also a highly symbolic

[56] See http://zone-h.com/archive/notifier=fux0r%20Inc

target and relates directly to the slogan in the first logo “Bringin’ the Peace of Mind”.

The content of this defacement is centred around the memory of the victims, with the first line stating that 9/11 is “a day that will live in the memories of this generation as well as those yet to come”. While the remainder of the text is largely a call for peace through US domination, the part which aligns web defacements with a struggle over public debate is found again towards the end where fux0r Inc. addresses the owner of the defaced page:

> anyway, sorry i dfaced this site even though the times make it that much more un-kosher. but they will occur towards every nation, because they are not an act of hostility, but instead to be thought as information insemination in the consideration for the regulation of the degredation of all great nations.

Similar to what will be discussed in relation to the WikiLeaks defacements in Chapter 7, defacers often have a clear understanding that they at least bother the legitimate owner of a defaced domain. This conflict is negotiated here by explaining that defacements are not an act of hostility, but rather tools to spread information. Noteworthy here is the acknowledgement that defacements during times of crisis are deemed more inappropriate in the eyes of the defacer. This acknowledgement hints at the core issue of the 9/11 themed defacements. Throughout this thesis, much has been said about the role of the knowledgeable underdog, that defacers regularly claim for themselves. In this role, defacers speak from outside mainstream society, using irregular channels of communication such as defacements, to be able to say all the inconvenient truths society needs, but does not want, to hear. While this promise of correcting public debate through bypassing gatekeepers is not always fulfilled, it is central to the self-understanding of defacers and is found time and again in defacements. But how could this role be translated onto the situation 9/11 presented? What could a defacer have to add to the discussion that had not already been featured in the extensive public debate in the weeks and months following the attack? In addition to this, as fux0r Inc. recognised, defacements of US pages would likely not be seen as expressions of solidarity but as nuisance or cyberattacks. In a time where allegiance and solidarity are public virtues, the eternal rebel defacer had to reinvent himself.

One possible way for defacers to remain in their familiar role of the outsider being right where the mainstream media is wrong are, especially in relation to 9/11, is in using alternate explanations or conspiracy theories. However, even discussions about what really happened on 9/11 were so popular that there was little need to discuss them on defaced websites. After the 9/11 commissions report was released, the topic gained traction and was the topic of many online debates (Pedersen 2013; Wood and Douglas 2013; Stempel, Hargrove, and Stempel 2007). However, the report also was not released until 2004, meaning that there was not much official explanation of the events to rebel against at the time of these defacements (National Commission on Terrorist Attacks Upon the United States 2004).

Another mechanism for defacers to produce themselves in the knowledgeable underdog role is of course the political fallout of 9/11, ranging from the suspension of civil rights to the suffering and death of hundreds of thousands of humans during the invasions and occupations that followed.[57] Here, hacktivism and defacements could play on their strengths as correctives of dysfunctional media and apathetic public. However, this fallout had just begun when most of the 9/11 defacements were submitted. The invasion of Afghanistan officially started on the 7th of October 2001, two days after fux0r Inc.'s defacement (Tomsen 2013).

The content of the defacement reflects on a double function it attempts to fulfil. One the one hand, it is the reaction to an unprecedented event in the life of most people, on the other it is an attempt to return to a normal flow of information and to re-establish previous hierarchies. As one section reads:

> also i just had to do something to bring back a lil feeling of normalcy.. been friggin wiggin.. they[the defacements]'re done in the honor of those innocent whom have lost their lives to ignorance in any country

The idea of bringing back normality through defacements is what connects many of the defacements in the 9/11 cluster, be it in an attempt to replay and overcome trauma or be it in the belief that peace could be achieved through US global hegemony. What brings many of these defacements together is a desire to go back to what was perceived as a better, prior state understood as normality. This is typical as part of a process of accepting change and loss – although it should be mentioned that no defacement in this cluster refers to a personal experience with the events on 9/11. Fux0r Inc.'s second line hints at some process that has been made in the Grief Cycle.[58] In dedicating the defaced pages to the memory of the victims, a bit of acceptance shines through and the first step towards the desired normality may have been undertaken. This defacement is indicative of this shift away from defacements negotiating the initial shock of the event to defacements attempting to process and accept the events.

Grieving is a well-established process in human society. Rules vary, but there are accepted places, occasions and rituals to express grief. While it is somewhat understandable that a defacer would express grief through defacements, it is hard to image that either the dispatchers, relatives of victims, or the general public appreciated the way grief was expressed here. Connecting to previous debates about whether defacements are addressing a circle of insiders such as like-minded hackers, or are messages sent out to a public sphere, 9/11 memorial pages are special in that their disruptive nature is incompatible with an empathetic message of shared grief or solidarity. Defacing a US website to express solidarity with the US public is not likely to have the intended effect, meaning that the defacements

[57] September 2021 estimates give the figure of 897,000-929,000 overall deaths in all post-9/11 wars, 363,939-387,072 of which being classified as civilian (Crawford and Lutz 2021).

[58] The Swiss psychologist Elisabeth Kübler-Ross defined five stages of grief: Denial, Anger, Bargaining, Depression and Acceptance. The stages are not part of a linear sequence but can be experienced in parallel with varying intensity (Kübler-Ross 1997).

in this cluster most likely had their most significant effect on the defacement scene itself, even though they appear to be directed outwards.

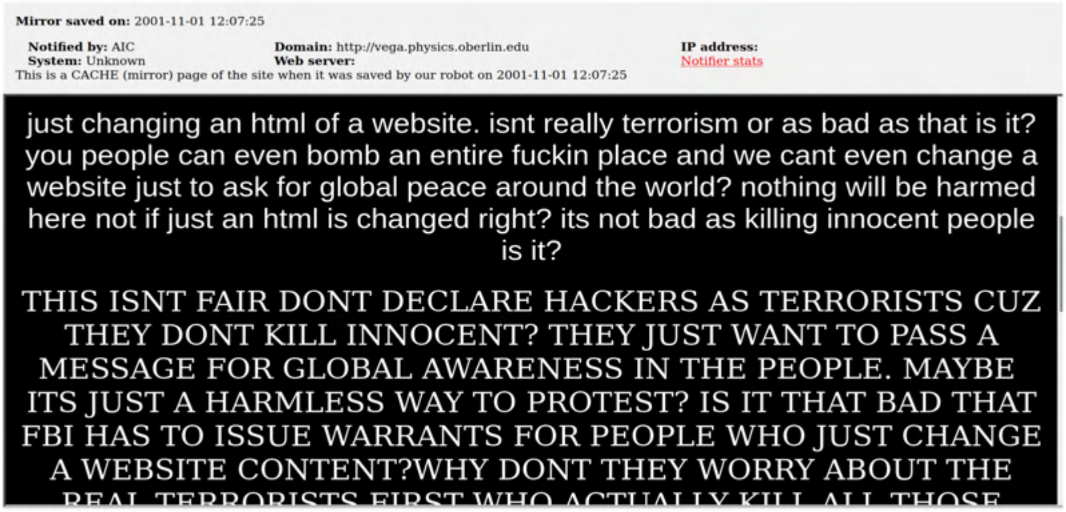
What makes the 9/11 defacements so special is exactly this conflicting situation it throws defacers into. The attention economy markets are in turmoil. The usual way of presenting is – at least temporarily – inopportune and new niches have to be carved out. However, to remain silent would mean to lose value in an attention economy scenario. Samuel comments on hacktivist’s – including, but not limited to defacers – assumed connection between tactics and awareness:

> The focus on audience, rather than speech, is clear from the comments of hacktivists themselves, who believe that their tactics translate into audience and awareness. [...] A member of the Electronic Disturbance Theater said that her group was “forcing people to pay attention” in a climate in which the “attention span is a minute.” (Samuel 2014, 212)

The attention span in the immediate post-9/11-period is close to zero for anything but the attacks and thus the translation from tactics (defacements) to awareness no longer functions. Some groups such as Bl4F and AIC attempted a return to the old ways by critiquing the legal fallout, but the statements they made were overshadowed by the more pressing need to first make sense of the events and images. Others, like fux0r Inc. attempt to use defacements as places of memory and seek close alignment with the US public, even though this puts their mode of communication at odds with the message they are trying to send out.

6.7.2 “*We are harmless*”

The type of defacements to be discussed in this section is a subset of the second category described above. This set is composed of defacements that happened in the months following September and on a surface level appear to be statements condemning terrorism.



Mirror saved on: 2001-11-01 12:07:25

Notified by: AIC **Domain:** http://vega.physics.oberlin.edu **IP address:**
System: Unknown **Web server:** Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2001-11-01 12:07:25

just changing an html of a website. isnt really terrorism or as bad as that is it? you people can even bomb an entire fuckin place and we cant even change a website just to ask for global peace around the world? nothing will be harmed here not if just an html is changed right? its not bad as killing innocent people is it?

THIS ISNT FAIR DONT DECLARE HACKERS AS TERRORISTS CUZ THEY DONT KILL INNOCENT? THEY JUST WANT TO PASS A MESSAGE FOR GLOBAL AWARENESS IN THE PEOPLE. MAYBE ITS JUST A HARMLESS WAY TO PROTEST? IS IT THAT BAD THAT FBI HAS TO ISSUE WARRANTS FOR PEOPLE WHO JUST CHANGE A WEBSITE CONTENT?WHY DONT THEY WORRY ABOUT THE REAL TERRORISTS FIRST WHO ACTUALLY KILL ALL THOSE

Figure 6.12: DefacementID 382, cropped

The screenshot is the second half of a text that begins with:

> Whateven happened on 11'th was Terrorism. Innocent people were killed we condemn that and we feel sorry for all those who died and we pray for their souls and their families.

The text then continues on by drawing parallels between the suffering of civilians in Afghanistan (during the invasion) and New York before arriving at its core issue which is shown in the screenshot: AIC, the group behind this defacement, protests being seen as terrorists due to their web defacements. The author argues that web defacements are just a harmless way of protesting and explains that no harm is done to the target system. Structurally, this defacement follows the known tripartite structure of a header introducing the group which reads:

> Supporting the same cause another website hacked by AIC (Anti india Crew)),

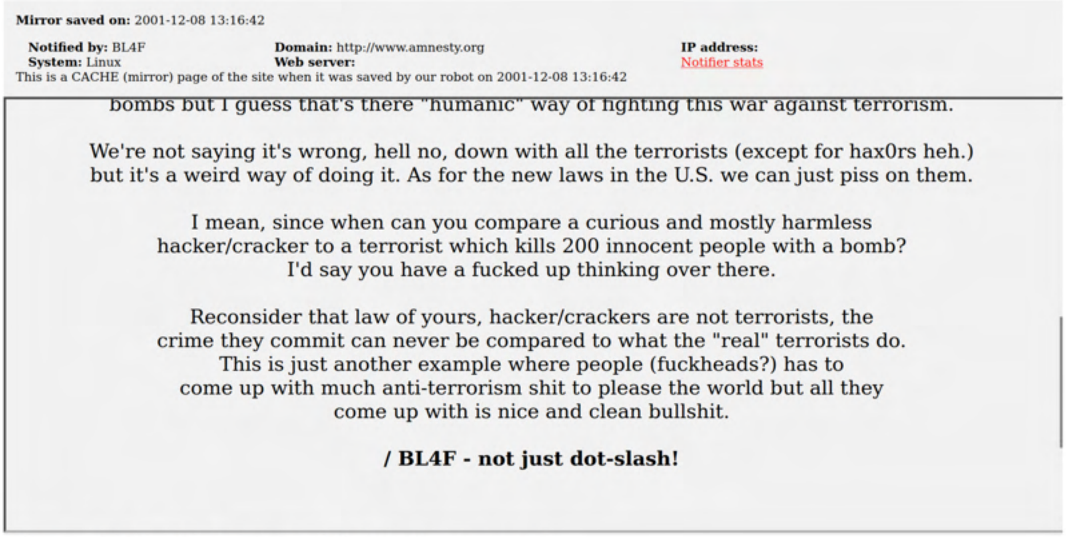
followed by the main body of the defacement, and then greetings to other defacers

> (SHOUTZ to everyone with the similar cause GFORCE,PCW,PHC,WFD and everyone in #a-i-c who support us and SPECIAL THANKS to Linux_Gal and Th3angel of AIC and my lovely friend [Grrl] and my man nul| !)

This acknowledging of other sympathetic groups such as GForce is a quite typical structure and signals that the mentioned groups were themselves campaigning against the cyberterrorist label. There are no pictures in this defacement and the text is kept to white on black background. The change in capitalization may suggest that the text was copied from different sources and compiled for this defacement. Also, the usage of a negative auxiliary verb construction as a rhetorical question

> (just changing the html of a website. isnt really terrorism or as bad as that is it?)

is not typical for AIC's style as seen in the Kashmir defacements.



Mirror saved on: 2001-12-08 13:16:42

Notified by: BL4F **Domain:** http://www.amnesty.org **IP address:**
System: Linux **Web server:** Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2001-12-08 13:16:42

bombs but I guess that's there "humanic" way of fighting this war against terrorism.

We're not saying it's wrong, hell no, down with all the terrorists (except for hax0rs heh.)
but it's a weird way of doing it. As for the new laws in the U.S. we can just piss on them.

I mean, since when can you compare a curious and mostly harmless
hacker/cracker to a terrorist which kills 200 innocent people with a bomb?
I'd say you have a fucked up thinking over there.

Reconsider that law of yours, hacker/crackers are not terrorists, the
crime they commit can never be compared to what the "real" terrorists do.
This is just another example where people (fuckheads?) has to
come up with much anti-terrorism shit to please the world but all they
come up with is nice and clean bullshit.

/ BL4F - not just dot-slash!

Figure 6.13: DefacementID 2940, cropped

This second defacement by BL4F (Figure 6.13) follows a similar structure of opening with an anti-terrorism statement to then turn to the criminalization of hackers. At its core is the same message sent by AIC that hackers and defacers are harmless and their prosecution is a waste of resources. Further similarities are the tripartite structure of the defacement with a header attributing the defacement to the group, a body with the main message and a footer. Further, both sites were defaced late in the year – November December 2001 respectively – and both target sites are high-value targets. The defaced pages belong to a college in Ohio and Amnesty International. Apparently being aware of the symbolic effect of hacking the web presence of Amnesty International just a few months after 9/11, Bl4F added a disclaimer at the bottom of the page stating:

```
We didn't touch the other domains such as www.stoptorture.org and
the old site is <a href="index.old">here</a> DS.<br>
```

This communicative strategy is coherent with observations which will come up again in the WikiLeaks chapter. Just like defacers expressed solidarity with WikiLeaks while defacing their sites, BL4F here makes the attempt to express their support of Amnesty's work by providing a link to the original page and stating that stoptorture.org has not been defaced. This shows, as in the WikiLeaks case described below, how freedom of expression and competition in the attention economy collide and force defacers to make compromises and apologies. The at times clumsy way political alignment is displayed in these defacements is rooted in the fact that defacers are making their point through the hack but are still demonstrating their general alignment with the principles of the target site. Defacers attempt to resolve this conflict by upholding a form of digital non-violence where they stress the harmlessness of their defacements.

In terms of style, both defacements show a high level of anger and estrangement expressed both in the choice of language and, for AIC, the writing in all caps. Both address a US-American audience with explicit referrals to “that law of yours” meaning the US Patriot Act. The practice of defacing web pages in reaction to legal proceedings against hackers is not novel to the 9/11 cluster, in fact it is one of the oldest recurring themes within the hacking community. The arrest of hacker Kevin Mitnick and the five-year-sentence he received sparked outrage and caused multiple defacements in 1995[59]. To trace the phenomenon back even further, even the 1986 Hacker Manifesto, a text distributed through newsgroups at the time, features the problem of prosecution:

> Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...
>
> Damn kids. They're all alike.
>
> But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
>
> I am a hacker, enter my world… (The Mentor 1986)

This understanding of being unreasonably criminalized feeds into the image of the outsider, the misfit rejected by society for exposing its true nature. The uniqueness of the 9/11 cluster defacements lies in their reaction to this type of persecution.

Instead of appreciating this reinforced outlaw status, AIC and BL4F chose instead to deface web pages to emphasize their harmlessness and to express their disapproval of being branded terrorists of any kind. Both lead into this topic by first distancing themselves from what they perceive as “actual terrorists” and then continue to describe web defacements as “just a harmless way to protest”. The key observation from the 9/11 defacements is that the attacks are such a shock to the defacement scene that groups need to reconfigure their image and communicate it through new defacements. As mentioned in the definition of web defacements, they are situated on an axis of transgression between civil ways to protest online such as campaigns and hashtags and hacking with the aim of disabling infrastructure, cyberterrorism or inciting violence. Through the above defacements, the definition is confirmed in that both groups take great effort to maintain that division between illicit but harmless web defacements and (cyber)terrorism. This shows that these dividing lines are well known to defacers and a vital part of how they see themselves and how they expect the public to see them.

These reactions, though, are a clear break from the 1986 and 1995 attitudes towards hacking which were anti-corporate and anti-governmental control of

[59] See the original US Attorney’s Office press release (United States Attorney’s Office 1995). Mitnick himself became a security consultant and author upon release. For a subjective account of his career, see Mitnick and Simon (2011; 2005).

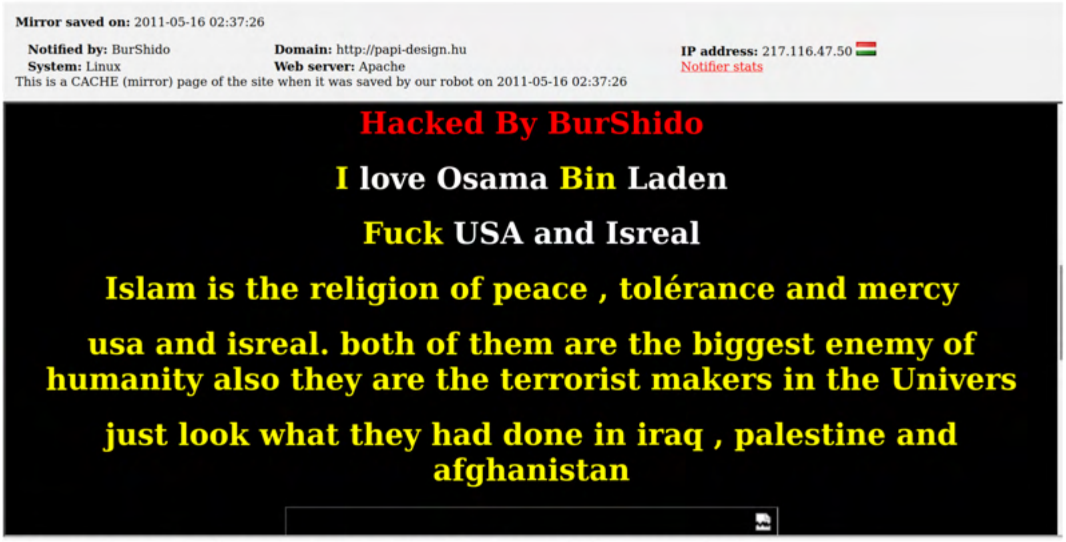
cyberspace. What AIC and BL4F show here is a close alignment with the causes of the US in the months post 9/11. It is not a discussion of the War on Terror and the – still ongoing – suffering of civilians in Afghanistan and elsewhere brought about by it. It is not the rejection of the unjust laws of an unjust society the hacker rebels against. Rather they offer an appeal to authority that defacers are harmless and not worthy of prosecution or close scrutiny. This went so far that even groups with a clear focus such as the Anti-India-Crew felt the need to weigh in on this topic.

The way this appeal is formulated and communicated to the audience is not without irony (defacing pages to say defacers are harmless) and reveals a lot of contradiction in defacement groups. It shows that amongst the whole underground aesthetic is a desire to communicate with the resented mainstream culture. This is probably best shown in the BHS interview where defacements are mentioned as a way of getting into IT security jobs (SilentStorm 2002). It further shows that despite the dramatic appearance of some defacements, and claims to be out of reach of any prosecutors, defacers see their work as of limited effectiveness and are aware of the dividing line between themselves and more destructive hackers

The defacements in this cluster appear to be anti-terror statements, but upon closer inspection reveal themselves to be details of defacer's programs and ethics. The aftermath of 9/11 made groups feel the need to distance themselves from any form of terrorism and publicly declare their harmlessness. This represents an interesting break from the usual image defacers like to cultivate for themselves and shows a move away from the hacking ethos of the 1990s.

6.7.3 Dishonourable Mentions: The long tail of 9/11

It was mentioned in the beginning of this chapter how the peak of defacer activity regarding 9/11 was between October and November 2001. There are, however, a few outside this time-line which can be described as the long tail of the 9/11 defacements. Partially owing to the collection process which ended systematic capture after December 2001 and only collected 2000 random defacements after that, not much relevant material has been collected. What has been collected is mostly on the borderline of the definition of political web defacements and only uses 9/11 as a starting point for anti-Semitic conspiracy (DefacementId 2940), or critique of the Patriot Act and other US surveillance programs (DefacementId 9705). Only one defacement indirectly expresses support for the 9/11 attacks:



Mirror saved on: 2011-05-16 02:37:26

Notified by: BurShido
System: Linux
Domain: http://papi-design.hu
Web server: Apache
IP address: 217.116.47.50
Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2011-05-16 02:37:26

Hacked By BurShido

I love Osama Bin Laden

Fuck USA and Isreal

Islam is the religion of peace , tolérance and mercy

usa and isreal. both of them are the biggest enemy of humanity also they are the terrorist makers in the Univers

just look what they had done in iraq , palestine and afghanistan

Figure 6.14: DefacementID 14040227, partial screenshot

Interestingly this is also the last defacement in the 9/11 cluster, submitted on the 16th of May 2011, shortly after Bin Laden's assassination on the 5th of May of the same year (A. Rogers and McGoldrick 2011).

These defacements form the long tail of dishonourable mentions since they contrast the authentic shock and – albeit – clumsy expressions of solidarity seen earlier. The three defacements described here were submitted by groups not present in the first wave of defacements during September and October, 2001. They are signs of a re-normalization of the attention economy where 9/11 has become just one of many topics. With this, they also represent some kind of closure in the grieving process, although it is not the original 2001 defacers like AIC and BHS talking here.

In this contract of voices, a strange diversity amongst the web defacement scene can be observed, where political content is superseded by technical practice. Samuel made the observation that:

> hacktivists often seem to shop for a political agenda after they have already made the decision to become hacktivists. This is evidenced by the fact that hacktivists define their movement not by its goals, but by its methods (Samuel 2014, 105)

Drawing on the findings from the 9/11 cluster, this assessment is confirmed. Web defacers have a clear focus on technical expertise – evidenced by the many disdainful mentions of script kiddies[60] and the focus on high-value targets – and base their reputation on it. Regarding content, anything goes, even non-content such as simple "hacked by X" messages. Defacements offer a scene which appreciates expression for its form, not for its content.

[60] A Script Kiddy is a hacker who lacks the skills to develop original attacks and instead uses (pre-made) programs and scripts to compromise a system ('Script Kiddy' 2018).

6.8 Conclusion

9/11 is an exceptional event in the context of the study of defaced websites. Suddenly and unexpectedly, it shook the attention economy and forced defacers to rethink their identity, strategy and audience. A survey of submission dates has evidenced a significant delay between the event and the peak volume of defacements. A study of the different types of defaced pages has shown this delay to be partially rooted in different motivators such as expressions of shock or protest against anti-terror legislation. The thesis that defacers pick their targets deliberately was substantiated by a comparison of the TLD profile of pages attacked by the same group in the context of the Kashmir conflict and 9/11. A clear focus on US-American domains could be shown for 9/11 related defacements.

The study examined primary material on the most active defacer group in the cluster, BHS, and traced its use of state symbols in defacements to establish a basis for understanding claims to national causes and expressions of solidarity. Following on from this, categories of defacements were described which ranged from expressions of grief to condemnation of the attacks to critiques of harmless defacers being labelled terrorists. As the immediacy of 9/11 subsides, the topic becomes merely one of many that defacers may use for political messages.

The impromptu responses and the lack of well-defined political standpoints by defacers brought up the question again of whether defacements are communicating outside the scene through their content or whether they are formalized expressions aimed at a scene recognizing them for their technical expertise. In reference to the genealogy of hacktivism, the performative aspect of defacements was stressed and related to Deleuze and Guattari's (1987) concept of (digital) nomads occupying the striated space of the web.

The significance of the 9/11 defacements lies in the contrasts and contradictions found. The data shows a clear alignment towards a US-centered, western perspective on media and politics which is at odds with the usual image of defacers as rebel outsiders. The primary data instead shows defacers as actors in an attention economy where knowledge about targets and attacks is an asset to be produced and invested. When the attacks of 9/11 occupied all public attention, defacers changed their approach accordingly. The lack of clearly defined political perspectives and the focus on the performative hack is complemented by a thrown-together assemblage of more of less politically charged phrases. It is the struggle of the nomads to define their standpoint in a suddenly smoothed digital space. This struggle only intensified when another actor upset the balance of the attention economy.

7. WikiLeaks and Defacements

7.1 Introduction

The purpose of this chapter is to provide a short historic overview of engagement with WikiLeaks in the web defacements analysed as part of this study. It was initially assumed that the release of the Iraq War Logs in 2010 would have provided a renewed interest in the conflict both from the side of defacers, media and general public and provoke wide engagement with the WikiLeaks organization. However, this was not evident in the dataset. In the absence of the expected wave of defacements, this gap in the archive offers the potential to give more insight into the scene and its use of information.

It might seem strange to devote a chapter to a basically absent phenomena, but rather than desperately searching for connections to fulfil a priori assumptions, this section is expanding the analysis performed in previous chapters as well as building on theories of attention economy established in the literature review. The relatively few findings in the archive allow for this section to function as a bridge between the case studies and the conclusion while advancing concepts of public, the value of information and the competitive nature of web defacements.

There is very little material found in the Zone-H archive relating to WikiLeaks. It was assumed that the Iraq War logs release from 2010 would spark a considerable number of defacements drawing on the information it released and the ongoing controversy of the leak, so the developed web crawler was used to capture defacements from the 22nd of October – the day the documents were made public. This crawl saw a very high density of defacements submitted daily, yet none were in scope or referencing WikiLeaks in any form. This is surprising considering the magnitude and scope of the documents released, providing details of 109,032 deaths in Iraq, 60% of which were civilian (WikiLeaks n.d.).

No defacements have been observed which used information from the Iraq War Logs in an argument against the occupation of Iraq. Also, no defacements were observed arguing in defence or condemnation of the leak campaign; the topic is simply absent from the archive. Further, there no defacements were observed arguing for or against or engaging in any form with WikiLeaks. Some hypothesis derived from this observation are explored in the following:

It is possible that the absence of any material is due to web defacements no longer being extensively used for political expression. This is likely not true, as the findings with the core data of this study show political defacements post 2010 and also other authors describe the ongoing use of web defacements for political purposes (Balduzzi et al. 2018, 25).

It is possible that there simply was not enough interest in the topic for defacers to engage with it. This is not to say defacers did not care about it. Rather, my suggestion is that the Iraq War Logs received so much attention from established media outlets that there was no need to repeat the same information on a defaced site. Public opinion of the time understood the leak largely as a justified action, so there was not much opportunity to reproduce one's own image as the knowledgable underdog defacer. This hypothesis is based on the assumption that, in order to stand out, the content of a defaced page has to be controversial similarly to the act of gaining unauthorized access to the site in the first place. In the case of the Iraq War Logs, there simply was no gain in repeating what the main television networks had already said about it. This hypothesis, though, is contrary to the findings in the previous chapter, where the events of 9/11 saw extensive coverage in defacements.

Lastly, the lack of material here might be attributed to the politics of the platform. As all submissions require approval to be included into the archive, it is possible that Zone-H staff decided to not allow defacements relating to the Iraq War Logs. This hypothesis is hard to substantiate, however the topic of WikiLeaks itself was addressed in an article published on Zone-H on December 2010, on occasion of the release of US diplomatic cables through Chelsea Manning. The article does not offer much detail about Zone-H's role (if any) in the release, but starts with a general statement:

> First of all, we would like to emphasize that Zone-H is not related to any party in the Wikileaks case. We are do not agree nor disagree with any action happened, we just want to share our opinion on the forthcomming events. Already many news media released information about the cables, sources, how it happened etc. (Minor 2010)

This statement indicates that Zone-H did not actively avoid the topic or ban it from its platform yet worked hard to distance themselves from it. It is hard to cross-reference the appearance of the WikiLeaks topic with other cybercrime archives, since only few of them remained active into the 2010 period. There is evidence, however, that Zone-H did avoid being too closely associated with WikiLeaks. This will be discussed further after the discussion of WikiLeaks-related defacements.

7.2 History

The platform WikiLeaks was first registered in 2006 as an "international non-profit organization working for transparency which publishes news leaks based on their ethical, historical and political significance" (Karhula 2012). The organization has been active since, with the most notable releases of information being the 2013 Snowden documents on US surveillance, and the 2010 Iraq War Logs, the biggest document leak in US military history.

As the introduction describes, there is reason to assume a cautious distance kept between defacement archives and WikiLeaks. To better understand why this distance exists between the two branches of hacktivist practice – web defacements and leaks – it is necessary to sketch out the historical development of both defacements and WikiLeaks. The time period in question lies between the start of WikiLeaks as a platform in 2006 and the Iraq War Logs of 2010. In the context of providing a historic development of WikiLeaks and its relation to hacktivism and, more specifically, web defacements, this section is concerned with how WikiLeaks position itself in relation to established and underground media.

Throughout this thesis, it has been proposed that web defacers are in a constant flux between private and public communication. Discussions about the nature of cybercrime archives and the analysis of the different parts of a typical web defacement reflect the often complicated condition of speaking privately to an in-group and speaking publicly to a public sphere. This hypothesis can be extended to WikiLeaks' complicated relation to other, mainstream media. Observers have noted how WikiLeaks' relation to media shifted in what I argue is a response to the complications brought about by this dual mode of simultaneous private and public speaking as well as in response to pressure put on the organization:

> WikiLeaks has gone through a series of metamorphoses: from a small, relatively unknown website devoted to giving whistleblowers space to release their material to one of the best-known activist organizations in the world. In addition, it has gone from being an organization that began by operating as an alternative to the mainstream media, to one that worked with the mainstream, and then to a group that devoted a fair degree of energy to attacking the media. (Christensen 2014b, 274)

This changing role of WikiLeaks from an outlet to a publisher is confirmed by Cammaerts:

> WikiLeaks decided to change its strategy from relying on alternatives to adapt more to the media logic, even if that entailed relinquishing some of its principles. The collateral murder video[61] is a good example of this. Instead of releasing the raw footage, WikiLeaks decided to edit the footage in order to increase its impact, subtitling what was said and adding a provocative quote of Orwell on the deceiving nature of political language. In doing so, WikiLeaks reneged on its promise to publish material as they received it and started assuming an editorial role and stance. (Cammaerts 2013, 431)

Both authors argue that WikiLeaks' relation to media has changed over time. This is important to understand any connections, or the lack thereof, to cybercrime archives and web defacements. Returning briefly to Zone-H's slogan "Unrestricted Information", and comparing it with WikiLeaks' approach to publishing content, we can begin to see how at the end of the first metamorphosis as described by Christensen, WikiLeaks and web defacements took different paths. The metamorphosis of WikiLeaks may be described as a change from Unrestricted Information towards Effective Communication. While the majority of defacements in the Kashmir cluster remains bound by the ideal of rationalized communication in a bourgeois ideal of the public sphere, WikiLeaks' media strategy had evolved to that of information capitalism, thus relying on supply and

[61] The Collateral Murder video was released in April 2010 and reveals the death of approximately twelve people, including journalists, in a helicopter ground attack (Dobson and Hunsinger 2016, 219). The video was one of the single most influential leaks on the platform. See also Christensen (2014a); Joanna Tidy (2017).

demand to determine the value of any item in public debate.[62] It has been described how many web defacements, especially up until the early 2000s, had a certain notion of objective truth as intrinsic value in them. While defacements continued to speak privately, expressing their subjectivity to a public carefully shielded, WikiLeaks saw information as a commodity traded on the true capitalist form of public sphere – the market.

In the Kashmir conflict cluster of web defacements, it has been shown how defacers struggled to convey their message when they relied primarily on the idea of unrestricted information. Unrestricted information in this case is the reproduction of one's own subjectivity, aimed at a well-defined group or scene. This mode of communication does not rely on the gatekeeping function of established media, because it was never truly aimed at any outsider. This condition is recognized and accepted by some participants in the cat-and-mouse game of web defacements, while others still struggle to convey messages they feel should genuinely be heard within the public sphere. In the early 2000s, when web defacers hacked pages to promote their share of information on the Kashmir situation, they found themselves in a situation where the lack of affiliation with established media came to be a disadvantage. Even if any number of web sites could be defaced, what would it matter against media empires and public indifference to the suffering of humans far away? Rationalized debate through information as attempted by these defacers is a kind of inward, private speech as it can only address those who already have said information or possess the capacity to obtain and verify them. Outward speech in the context of effective political communication is based on narratives and affective frames.[63] It is no coincidence that the second case study example from the Kashmir complex diverges from that strategy and uses one piece of information – rather than the plethora of information seen on other defacements – published on a well-known news website.

As further indication of how WikiLeaks and the majority of web defacements followed different strategies, WikiLeaks founder Julian Assange is quoted:

> You'd think the bigger and more important the document is, the more likely it will be reported on but that's absolutely not true. It's about supply and demand. Zero supply equals high demand, it has value. As soon as we release the material, the supply goes to infinity, so the perceived value goes to zero. (in Christensen 2014b, 280)

[62] This critique of the bourgeois ideal of the public sphere is described by Habermas in his initial work on the public sphere:

> Marx denounced public opinion as false consciousness: it hid before itself its own true character as a mask of bourgeois class interests. His critique of political economy was indeed aimed at the presuppositions upon which the self-interpretation of the public sphere in the political realm rested. (Habermas 1989, 124)

[63] For an introducing to the topic, see Herman and Chomsky (1988). More recent works on the topic include Cacciatore, Scheufele, and Iyengar (2016); Spence and Pidgeon (2010); Vliegenthart (2012).

This quote indicates Assange acting in a way opposite to the unrestricted information mantra of Zone-H and other cybercrime archives. Assange is fully aware of the market WikiLeaks is competing for attention on. His statement does not mention ideas of rationalized debate or the inherent value of information. Instead, the core of this attention economy is "supply and demand"; the market. In this political economy of information, WikiLeaks acts as an information capitalist creating artificial scarcity of information and using it as resource to gain the maximum profit. It also puts the later WikiLeaks approach of releasing selected pieces of information in cooperation with newspapers such as the *The Guardian* in opposition to most political defacements which attempt to put as much information as possible onto the defaced page, as in the first example of the Kashmir cluster. The two positions are opposed in that the latter relies on assumed shared ethical values while the former relies on the forces of supply and demand.

A brief return to the methodology section confirms much of Assange's statement. If it is assumed that most defacement IDs on Zone-H refer to a defaced page (some lead to defacements deemed invalid and removed), then the cybercrime archive holds upwards of 3 million defaced pages without any content-related metadata or search function. This is the equivalent of the infinite supply, zero value situation described by Assange. A good part of the methodology is concerned with making sense of this unordered pile of information, which, in mainstream media, is the part that would be played by journalists and editors. If that part is missing, the information is less restricted, but also less accessible. Unrestricted information is related to the technocratic order of society also expressed in open source where the published code is supposed to increase transparency for all while, in reality, it remains inaccessible for the majority of society who now have to trust the new gatekeepers (the programmers) to make decisions for them.

The point I am stressing in relation to a shared history between WikiLeaks and web defacements is that while both started out with similar ideas of unrestricted information, WikiLeaks eventually abandoned this for a more information capitalist approach. Information capitalism describes a fundamental change away from information as commons to information as resources, best depicted in the contrast between the hacker ethos of "information wants to be free" and Assange's declaration that attention is matter of supply and demand.[64] WikiLeaks also understood how to utilize established media to convey its message. In contrast, web defacements containing political expressions are most aligned towards the simple output of information, relying on the information's importance to create publicity. While there are differences between the nature of the two (most prominently the unexpected appearance of a defaced site while WikiLeaks is a

[64] Since digital information can be replicated at almost no cost, the idea that information should be freely available without restrictions has become part of hacker ethic. The slogan "information wants to be free" was first attributed to Steward Brand, founder of the *Whole Earth Catalogue,* in 1984 (Clarke 2004). Richard Stallman, founder of the GNU free software foundation, uses the slogan in his writings on free software (Stallman and Gay 2002).

more steady object), and while it is hard to summarize all web defacements as guided by the same ideology, it can be noted that the two forms of activism took different paths. This difference is reflected in their structure and content, with only occasional overlap.

7.3 Findings in the archive

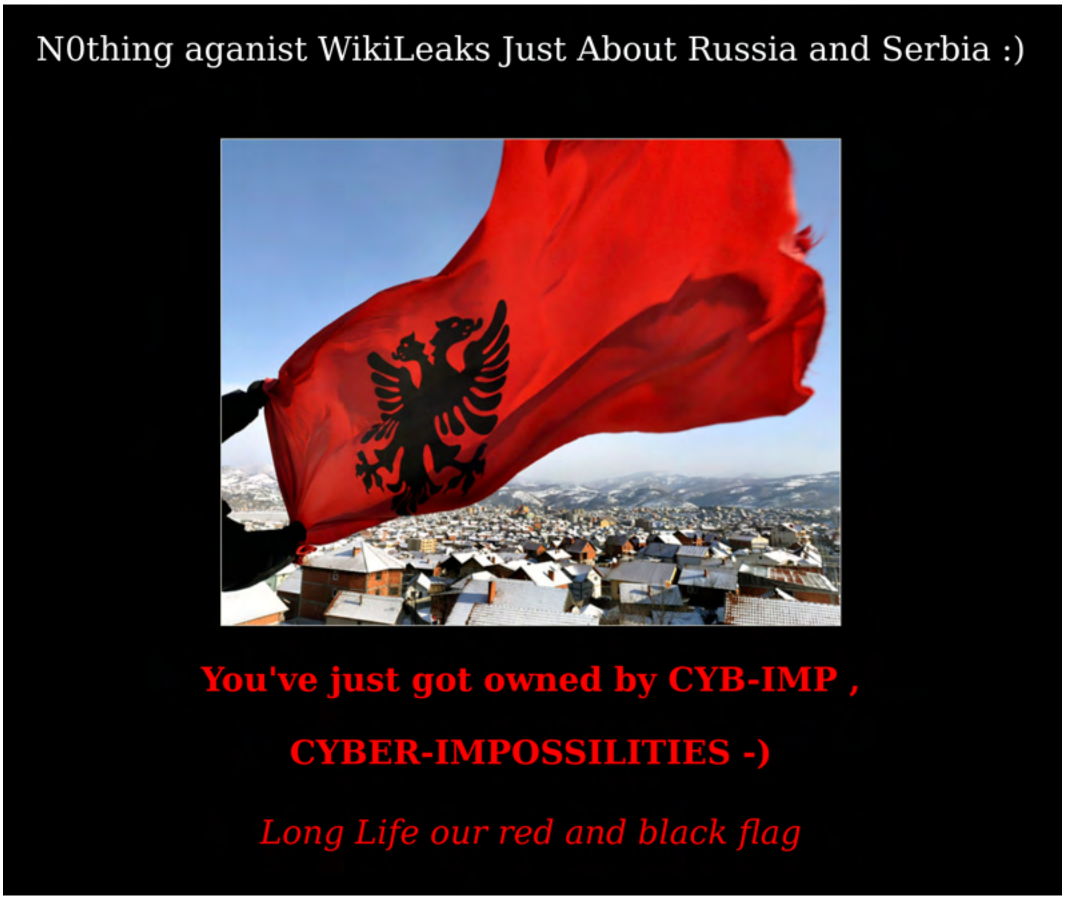
As already indicated, the lack of material on WikiLeaks' activities in the data set is striking. There are, however, a few defacements engaging with WikiLeaks present in the archive. Owing to the structure of the archive (no full text search or tag search of any of the defacements possible) the user can only search by domains or by notifier name. Searching for WikiLeaks-related domains returns a few cases where local WikiLeaks domains were defaced. Three of these defacements will be discussed in detail as they provide insight into how the defacement community engaged with the topic of WikiLeaks. It is important to understand that while these defacements engage with the topic, they are not used to promote WikiLeaks in any way nor do they attempt to raise awareness about the site. In reference to earlier chapters describing hacking as a critique of technology fuelled by a technocratic utopian vision, those defacement are artefacts produced by a critique of technology which prove that debates on how WikiLeaks should operate extended into the defacement scene.

The first defacer engagement is a 2011 defacement of Wikileaks.hr, a Croatian spin-off.[65] The domain is not listed on the official WikiLeaks mirror list (WikiLeaks n.d.), so it could not be confirmed to what extent the page was affiliated with the original Wikileaks.org domain. Nevertheless, this defacement is emblematic of a kind of engagement with WikiLeaks that attempts to profit from the site's popularity. In this context, it seems that WikiLeaks.hr was simply a high-value target. The defacer did not leave behind any specific message and did not engage with the original page material in any way. The defacer had been submitting defaced pages from 2010 to 2013, with some of the earlier submissions expressing anti-Israeli positions and expressions of solidarity for Palestine. Whether or not WikiLeaks was chosen in this context is impossible to say from the evidence. Against this assumption speaks the fact that no specific message was left. The other sites defaced by this attacker seem to be much less controversial than WikiLeaks and were likely chosen for ease of access.

The second noteworthy incident is the August 2011 defacement of Wikileaks.ru, a Russian version of the original site.[66] Here, the defacer expresses an interesting mix of conflicting interests:

[65] DefacementId 14311610, 2011-07-01 Wikileaks.hr was overwritten by an unrelated message.

[66] The site has since gone offline, but a July 2011 snapshot exists: https://web.archive.org/web/20110718081804/http://ru-wikileaks.ru/



N0thing aganist WikiLeaks Just About Russia and Serbia :)

You've just got owned by CYB-IMP ,

CYBER-IMPOSSILITIES -)

Long Life our red and black flag

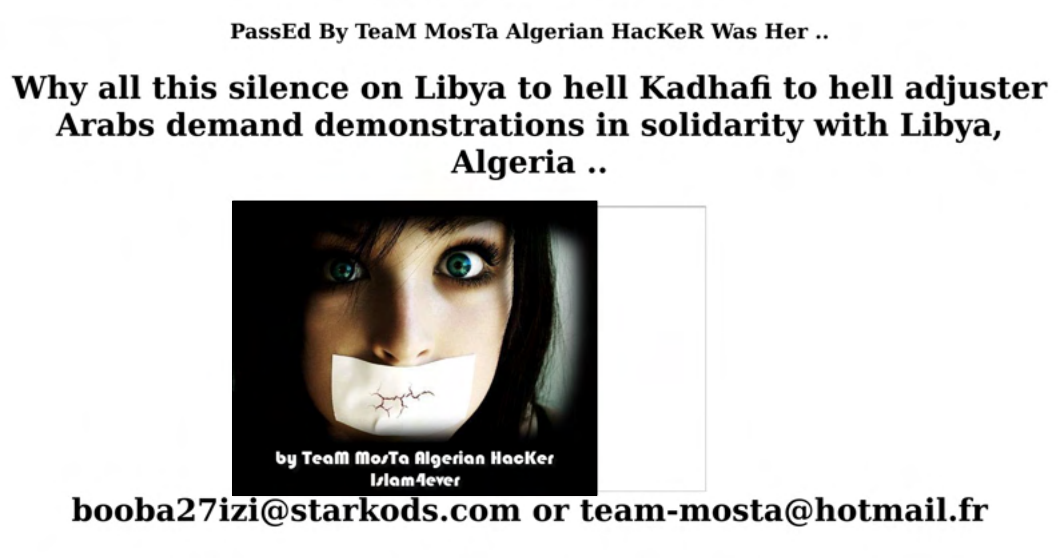
Figure 7.1: DefacementId 14606547

The settlement behind the Albanian flag in the image is supposedly the town of Mitrovica in Kosovo. The area saw tensions rising during the 2011 to 2013 North Kosovo Crisis. This defacement is part of a series of near-identical defacements, but with the addition of the dedicated message to wikileaks.ru. The statement shows that CYB-IMP was well aware their defacement could be understood as an attack on WikiLeaks itself, which they in turn tried to preempt. It also shows the defacer’s priorities in carrying out the attack anyway which are to gain notoriety within the defacement community. This defacement also follows the header-message-footer layout, featuring a shout-out to the community at the top and the mentioning of the defacer at the bottom.

In this example, various interests intersect: the communicative function of this defacement is not primarily in what is said on the page, it is the whole context of where and when the text is inserted. This defacement would not work on, say, an Italian website (for the lack of audience) whereas most of the context seen in the Kashmir cluster bears no relation to the target page. For the statement to function, a Russian or Serbian site had to be targeted. Wikileaks.ru might have come into focus for the same reason wikileaks.hr did: because it would receive a high number of clicks from Russian visitors and thus was a high-value target. What sets this one apart from the first WikiLeaks-related defacement is the message left behind. In a typical fashion for defacements, the actual message is framed by an introduction “N0thing against WikiLeaks Just About Russia and Serbia :)”. This is supposed to contextualize the defacement of Wikileaks.ru and to assure the viewer that this site was not defaced in protest against its content, but in an attempt to virtually occupy a popular space. The practice of occupying and blocking access to a public space has a long history in physical protest and a somewhat shorter history in activism on the web (Lasn 2000, 133; Papacharissi 2010, 158; Cammaerts 2013, 421).

In this case, the defacer chose a page that was not just irrelevant to his interests, but one that – judging by the message – was at least considered worthwhile due to high interest. If this defacement were about information and/or propaganda, the argument could be made that Wikileaks.ru has more to offer than a nice picture of the Albanian flag. Also, as was shown, some defacers pride themselves in not damaging the target system and do not actually overwrite the website but include a link to the original content in their defacement. There is no reason the author of this defacement could not have done that, especially when there are apparent sympathies for WikiLeaks. What the whole defacement, including what this overwriting of the original content hints at, is a struggle for attention within the scene and between all online activists. Be it Wikileaks.ru or the defacer CYB-IMP, they are actors in an attention economy competing for limited resources. This competitive scenario mirrors observations made earlier about the inherent conflict between the value of free speech as valued by online activists and the meritocracy of cybercrime archives where the most skilled hacker may overwrite any text with any message. It connects to the attention economy described earlier in this chapter, where WikiLeaks was described as acting successfully in the role of an information capitalist. It further outlines the edges of the rationalized public sphere model upheld by much of the defacement scene in the early 2000s. Caught in a competitive scenario, the defacer abandons the ideals of rationalized discourse and instead utilizes his hacking skills as cultural capital to dominate the debate, at least momentarily. In this act, the promise of unrestricted information is broken and the public sphere of web defacers is revealed as a small-scale superstructure built upon the base of an attention economy.

A third defacement of a WikiLeaks domain mentioned in this context occurred in February 2010, when Wikileaks.ir was defaced with a very specific message:



PassEd By TeaM MosTa Algerian HacKeR Was Her ..

Why all this silence on Libya to hell Kadhafi to hell adjuster Arabs demand demonstrations in solidarity with Libya, Algeria ..

booba27izi@starkods.com or team-mosta@hotmail.fr

Figure 7.2: DefacementId 13140984, the image is not part of the original capture

The defacer, team-mosta, is an Algerian hacker collective active on Zone-H from 2010 to 2015. During this time, they submitted the impressive number of 19,958 defacements to the site.[67] Some of these defacements are devoid of political messages, other express sympathy with Arab struggles such as Gaza. It could not be determined if this defacement is part of a series or an individual piece, however judging by the specificity of the message it seems likely to have been written just for the WikiLeaks domain.

The domain itself appears to have been a localized WikiLeaks outlet and has since gone offline.[68] The defacement features three almost universally used elements, it frames the message with an introduction naming and introducing the defacer ("PassEd By TeaM MosTa Algerian HacKeR Was Her ..") before it moves on to the message ("Why all this silence on Libya … ") and finally brings the reader's attention back to the defacer by providing contact information. The image used in the original defacement was not captured by Zone-H's web crawler at the time, but could be retrieved through the Internet Archive.[69]

What sets this defacement apart from the first two examples of engagement with the thematic complex of WikiLeaks is the defacer's attitude towards the target. While in the first two cases, it was assumed that WikiLeaks domains had been chosen for their reach and the attention generated by them, this defacement is different in that it offers a clearly expressed critique of WikiLeaks. To be more precise, what is expressed here is not a fundamental rejection of WikiLeaks as a platform, it is a comment on the perceived lack of content regarding Libya. This

[67] http://www.zone-h.org/archive/notifier=TeaM%20MosTa

[68] For a capture from February 2010, see: https://web.archive.org/web/20110221153751/http://wikileaks.ir/

[69] https://web.archive.org/web/20110815000000*/http://www.filetolink.com/5812b998

contextualizes the defacement as recognizing attention as a limited but vital resource in hacktivism and thus seeing WikiLeaks as detrimental to one's own cause by absorbing too much public attention. The hacktivist solution is then to disable access to the domain and by doing so to promote their own cause while shutting down the competition. The defacer in this case is also acting as an information capitalist employing their capital to distort the market and limit supply. There is the impression that now (in the three defacements around WikiLeaks domains from 2010 and 2011), the notion of truth as key value in political communication has been replaced by a struggle for attention which cannibalizes sites that would otherwise be on the same side of the spectrum. Consequently, team-mosta accuses WikiLeaks not of lies, but of omission. It has been said before that it would have been easily possible to include a link to the original site and to use the defacement as a kind of unofficial addition to the original content. The same applies here and the fact that it was decided to completely overwrite the original content shows the much increased focus on attention as the main objective of a defacement.

All of the above three cases show different levels of defacer engagement with the topic of WikiLeaks. In the last two cases, it was apparent that conflicting attitudes between approval of WikiLeaks overall as a platform and the temptation of a high-value target for defacement exist. In these cases, the defacer attempted to negotiate this conflict through the messages left behind, although they appear as little more than excuses for the defacements.

What is striking, however, is the overall low number of defacements engaging with the topic of WikiLeaks and within that small section, the lack of content promoting or expressing approval for the platform.

It has been noted how a constant struggle for attention cannibalizes hacktivist' efforts to communicate effectively. This communication problem is due to hacktivists acting as information capitalists aiming to reduce supply and distort the market towards a monopoly. Referring to WikiLeaks and the discussed examples, this situation seems to have intensified during the early 2000s.

For Zone-H, the role of neutral observer had to be maintained particularly as WikiLeaks began attracting legal attention from US authorities. A search on the WikiLeaks website reveals 27 documents mentioning Zone-H explicitly.[70] In all cases, Zone-H is mentioned as a cybercrime archive holding a copy of a defaced page. It is never assumed or stated that Zone-H was behind the attacks. It is not hard to imagine how this represents a massive conflict of interest for Zone-H staff. On the one hand, their site being used for such hot political defacements is exactly what the site's public image is built around. On the other hand, how far does a volunteer-run collection of hacked websites want to be dragged into a conflict involving intelligence agencies and government-sponsored hacking teams? Even if Zone-H has nothing to do with the defacement itself, the fact that they act as an

[70] See https://search.wikileaks.org/?q=Zone-H

archive stabilizing the ephemeral object of a defaced web page makes them a multiplier in whatever message defacers decide to broadcast. This is confirmed as soon as Zone-H is quoted as the mirror of a defaced page.

There is another aspect to the relationship that explains the skepticism with which the topic of WikiLeaks is treated by Zone-H, and which potentially sheds light onto the seemingly difficult relation between the two. Returning briefly to the statement this chapter was started with, it appears strange that Zone-H would so strongly express their non-involvement in anything WikiLeaks related. Such a statement raises the suspicion that an accusation of being involved with or facilitating WikiLeaks was either ongoing or at least expected to be voiced soon. There is another statement which indicates that Zone-H was determined to not be associated as anything other than a medium. On the 22nd of November 2009, a post was made by one of Zone-H's admins regarding a leaked document featuring Zone-H:

> We received a notice that on WikiLeaks somebody uploaded an interesting document. It's a PDF file, called Project Ethan (after Tom Cruise's Mission Impossible caracther?) and it refers to E2-labs very recent plans to open in India an educational and IT security franchise network. We downloaded the document and we found some very interesting information in it, regarding E2-labs future plans and how the name of Zone-H (and a few others) was used to back up the whole plan to convince possible investors to invest money [...] Needless to say, Zone-H was never informed about such plans and never gave any consent to be included in it. (Preatoni 2009)

Again, while this expresses a recognition of WikiLeaks as a source and platform, it seems strange how this somewhat banal incident where Zone-H's name is used to gain some credibility to attract investors would spark such a response. The article is announced a few days prior and extended by author's additions and an email from one of the other organizations mentioned in the document.

The described incident seems to be a conflict between Zone-H and the organization behind the leaked document (E2-labs), with WikiLeaks only acting as the medium through which the information is passed. It is nevertheless noteworthy in this context because it describes how Zone-H navigates conflicting interests and offers a hint at the internal policies regarding WikiLeaks which are to display non involvement at all times. The conflict for Zone-H lies in a desire to stay relevant as a cybercrime archive while also not being too closely associated with the content and context of the submitted defacements. The E2-labs document might have simply been an unlicenced attempt to profit from Zone-H's reputation, but the site's reaction shows how steps were consitently taken to ensure Zone-H would be perceived as a neutral observer not invested into either WikiLeaks or E2-labs.

The situation is a double bind for the site. Continuing on, with an emphasis on neutrality and freedom of information, carries the risk of being seen as facilitating and encouraging hacktivism and eventually facing repressions similar to

WikiLeaks.[71] Implementing a policy with the aim to distance Zone-H from content deemed too politically charged carries the risk of losing significance as a source and losing credibility amongst the hacking community. If the aforementioned statements are anything to go by, the strategy was to attempt to find some middle ground by strengthening their role as neutral observer.

This double bind is representative of a larger debate amongst web communities in the early 2010s. This time frame saw a general discussion about the extent to which the providers of online communities could be associated with the content on their platforms.[72] The debate marked the end of an idea the mainstream held on to until its last breath: that digital communication was a separate sphere, free from hate and political agitation that plagued the offline world. While this is peripheral to the study, it is important to see how even a cybercrime archive had to engage with this debate and try and find its own answer to it. However successful the answer was, the bind Zone-H found itself in might be part of the answer as to why a topic of the magnitude of WikiLeaks only produced a handful of defacements and a few passing remarks.

The entire situation around WikiLeaks as described in this chapter is the acid test for the technocratic public sphere as envisioned by Zone-H and web defacers alike. To participate in it, a defacer needs the right kind of capital in the form of hacking skills and available time. To be heard, a defacer has to essentially deny freedom of online expression for as many others as possible. These factors describe the defacement scene as focussed inwards, with more or less clearly drawn boundaries. This complicates any attempt to effectively reach out and leads to a situation where defacers communicate amongst themselves to uphold the idea that their defacements are valid and effective tools of political participation.

The public sphere of web defacements – or the sphere of Unrestricted Information, as was Zone-H's slogan – does not exist in a vacuum, nor was it formed in a magical cyberspace realm far outside the reach of Realpolitik ideas. Engagement with the topic of WikiLeaks outlines two main characteristics, internally and externally of said public sphere. Internally, all participants are subject to the rules of an attention economy where supply and demand regulate the value of any piece of information. Consequently, successful actors are information capitalists, as may be seen in the Assange statement and the defacement of WikiLeaks domains. Externally, this sphere exists within other

[71] For an overview of measures taken against the continued operation of Wikileaks.org, see Cammaerts (2013, 429).

[72] See also Alexander and Alexander (2018); Hoeren (2009); Suzor et al. (2019). The movement to hold providers responsible for user content has been described as part of a "cascading hierarchy of surveillance":

> the most effective system of controlling the Internet [...] is the one that reproduces the time-tested method used over the years to control the media: the cascading hierarchy of surveillance that ultimately induces self-censorship at all levels, and makes the culprit pay at each level when a significant failure of control is detected. (Dong (2008), in Castells 2013, 283)

structures of power. When Zone-H stays suspiciously distant to WikiLeaks, emphasizing their non-involvement multiple times, it is in an attempt to naturalize the attention economy market and to position themselves as merely the conduit through which transactions take place. Both characteristics show the limits of the public sphere as constituted by the Zone-H cybercrime archive, firstly its dependence on the base structure of the information economy market and secondly its embedding in larger power structures.

8. Conclusion

8.1 Overview

This dissertation started with two goals. First, to undertake an academic web archiving project on vanishing defacement archives. Second, based on the archived material, to undertake a study of web defacements, defacer motivation and strategy. Both goals and the selected case study examples took the reader through a range of technological and sociological readings of web defacements as tools of political expression. This remaining chapter will now summarize the key findings of this study, but it will also address topics and questions that can only be dealt with by finding interlinkage between the chapters.

The project started out with a focus on the making, contesting and overwriting of public debate through defacements. This focus remains, but the experience of the research has shown that the way information is invoked, created and challenged through defacements is far more complex than initially thought. Electronically mediated information, and its connections to public space, materiality, hacking and subversion, are topics that were traced through all chapters, yet they benefit most from the overview perspective of the conclusion. As much as the term information has different meanings from a technical and a sociological perspective, and this project in its chapters has been switching between both, it is important to understand information as an element embedded in a process. Employing such a functional perspective shows that information in either sense of the word is framed as part of a larger process of meaning-making.

8.2 Hacking the Public Sphere

Framing the object and the objective in this study was done through different approaches in chapters 2 and 3. Chapter 2 established a taxonomy of hacktivism as a general category and went on to further narrow down a definition of political web defacements. This definition was then further described by adding the level of transgression as a qualifying feature. It was argued that political web defacements need to be more transgressive than netstrikes and other forms of civil engagement, yet less transgressive than forms of cyberwarfare. This helped to position political expression in web defacements and was important to define the frame of this study. Approaching political expression in web defacements from the perspective of a history of political engagement allowed understanding of web defacements as the evolution of methods to contest public space and public expression. The work in chapter 2 also mapped the history of hacktivism as a practice and its association with particular political positions - something that was challenged by looking at what defacers do as a transformation of the materiality of memory.

The objective, then, was to obtain a number of these expressions and analyse their relation to political expression especially relating to their perceived audience. It was the implied assumption that by engaging with and challenging information available to the public, these defacements attempted to act politically. However helpful such a framing is in approaching the object and objective, it must be acknowledged that any direct lineage between on- and offline political expression is at risk of overlooking the specificities of the medium it is dependent on and underscores the need to understand hacktivism as computer-aided activism. This process of framing in Chapter 1 already began to uncover theoretical blind spots in regard to web defacements and hacktivism as well as defacer motivation to engage in these potentially illegal practices. These were explored further in Chapter 3.

Chapter 2 reviewed the existing literature around the materiality of information systems and politics of the Internet. The goal of this chapter was to synthesize the at times very different concepts of hacking and hacktivism into a conceptual framework to describe and analyse political web defacements. What the analysis found was that hacktivism is often described from a technical perspective as illicit tampering with information systems without concern to actors and their motivations or as the continuation of offline activism happening through a digital medium. Both definitions paint an incomplete picture of the diverse motivations of hacktivists, the organisations within the scene and the inherent politics of the competitive situation web defacers find themselves in.

To better understand the notion of hacking as a worthwhile form of political expression in the first place, the chapter outlined a history of hacktivism tracing its influences from early computer culture and counterculture. It is from these two influences that the figure of the modern hacker as someone who successfully re-appropriates technology appears. It is also from these influences that a strong techno-optimism originates which is expressed in a computational mindset, where most conflicts present themselves as data routing and computing problems. This history of hacktivism is important to frame the expansionist and free-trade mentality which shapes hacking.

The rest of Chapter 2 then investigates the role of hacktivism and web defacements on a larger scale, describing its role in a Habermasian public sphere. As much as hackers are portrayed as individualist outsiders, the argument made here is that for many of them, web defacements seem to be gateways to a public sphere discussion they otherwise feel excluded from. The social capital required to partake in said discussion is the hacker’s skill and ability to deface pages. Of course, the very idea that defacers see their actions as aimed at a receptive public sphere reveals their alignment with Western liberal democracies more than with anarchic cyber-hedonism. This brings the analysis back to the very same cultural backgrounds which gave rise to the technologies and ideologies described in the history of hacktivism.

Chapter 2 so far has been concerned with the actors in web defacements, yet one of the blind spots in the review of the existing literature was a detailed description of the material these actors work with. This leaves the realm of digital activism and opens the scope to include processes of myth-making and archiving as ways to exercise power in a networked society. While a body of literature on this topic exists and has been consulted for the analysis, works on the specific conditions of memory mediated through digital networks as a site for subversion are scarce. After providing a history of hacktivism, Chapter 2 outlines how, through increased integration into the facilitating machines, information becomes machine-to-machine communication, only partially translated through an interface. The increased dependence of the medium on its technical infrastructure opens up a new site of subversion where the defacer may insert their own information into this memory-making process. With the framework built, the thesis is able to understand hacktivism through practice rather than ideology.

8.3 Building a Methodology

To translate and test the conceptual framework of Chapter 2 via a methodology appropriate to the distributed and hard-to-access collections of defaced web pages was the aim of Chapter 3. The methodology developed in this case had to overcome several of challenges owing to the nature of the material. The first of these was that no dedicated, comprehensive collection of political web defacements exists. No academically usable collection of web defacements is publicly available. Material to draw upon comes from large, community-run cybercrime archives. The first challenge was to identify relevant and still existing collections of web defacements. Following previous work on the topic and reconstructing mergers and disappearances of collections, Zone-H was decided on as the most promising object of study.

Zone-H holds well over three million defacements of various nature. The site allows only very limited access to its data and provides some metadata about the defacer and the time and target of the attack, yet no metadata about content or motivation is available. The site is served through JavaScript, so that off-the-shelf web crawlers are largely unusable. In a second step, the methodology applied had to account for this and effectively re-create an archive of political web defacements out of the deluge of hacked pages stored in Zone-H. To still be able to archive pages, I developed a web crawler using automated browsing to go through the collection and archive the defaced page, take a screenshot for easier classification and record any metadata that was available. This allowed the capture of most of the available material from the earliest defacements in 1998 until the end of the year 2001. After that, defacement numbers were so high that only random samples could be captured for the remaining years. A total of 12,000 pages were captured and processed that way. Manual screening revealed a low percentage of these pages fitting my definition of political web defacements outlined in the beginning of the study.

The analytical methods applied to the dataset had to be qualitative and fine-grained enough to be able to understand the often-diverse nature and motivation of web defacers, yet at the same time qualitative and broad for the study to introduce web defacements as an object of ongoing study. The chosen mixed-methods approach investigated web defacements in reaction to the Kashmir conflict and the 9/11 attacks, while also defining web defacer's relation to WikiLeaks to further position political defacements within a larger framework of hacktivism. The analysis also classified the entire dataset according to defacer motivation and mode of expression. This was done to include all voices in the dataset and to be able to map significant changes in the way web defacements function over time. There were severe ethical considerations involved in the choice of data, although this research did not involve human subjects in any way. These considerations were for the most part about the absence of confirmed informed consent both on the side of the defacer, the legitimate website owner and people whose images and data might be used in defacements. Ethics were discussed in detail throughout this chapter, as it is a complex topic showing itself at all stages of the design of this study.

8.4 Finding motivations

To understand how web defacements function and how that function has changed over time, Chapter 4 undertook the effort of tagging the entire corpus of the research dataset according to defacer motivation. Motivation was divided into ends-oriented, expressive, interactive and solidary incentives, whereby consideration was given to how these incentives overlap and contradict each other. The results have shown how heterogeneous and diverse defacements are. What unites most of them is a strong desire for interactivity through various elements commonly used on defaced pages, such as greetings or dedicated messages to fellow hackers. A noticeable shift in the tone of web defacements is found with 9/11, which gives rise to the memorial type of defacement which until then had only been used occasionally. Before September 2001, defacements as a whole are more designed to be discussion pieces in a Habermasian sense with an emphasis on providing as much information as possible. Defacers would openly express their allegiance with a certain hacker ethic in stating that no harm was done to the original site as well as in the political positions they adopt. Starting with 9/11 though, defacements tend to make more use of memorial pages, favouring narrative and affective appeals to mere information provision. These defacements are typically image-based and defacers are less likely to express either allegiance to hacker values or send a special message to the perceived enemy through the defacement.

Further, Chapter 4 also rebuilds metadata for defaced pages where possible and contrasts said metadata with Zone-H's own statistics. The aim of this attempt was to answer the question of whether political web defacers would prefer easy targets unrelated to their cause or more difficult to hack targets with a strong public profile. Although it was not always possible to directly compare metadata, the analysis nevertheless shows evidence of a target selection more focussed on governmental websites of any nature than the bulk of web defacements.

Finally, a part of the scope of Chapter 4 was to test an automated approach for the identification of topics in the research data set. As has been outlined in the description of the data source, political web defacements are usually held within larger cybercrime archives and hard to find due to a lack of metadata. To be able to continue research on web defacements on a larger scale such a data set is needed. Consequently, Natural Language Processing was used on the corpus to identify themes and commonly used expressions to create such a set and also to aid in the selection of material for the more focussed case studies. In this process, it was shown that Natural Language Processing is suited for screening a large number of HTML files for relevant content. This analysis also confirmed that the Kashmir conflict is the most prominent topic in the data set, and that 9/11 caused a significant spike in defacement activity. These two clusters in the data set were thus identified as case studies for the closer analysis of hacker activity.

8.5 Information and frustration

Chapter 5 provided a detailed study of web defacements submitted in relation to the Kashmir conflict. The chapter shows how defacers struggled to make their defacements a part of a public debate by providing information about ongoing developments and calling for support from their audience. The role defacers saw for their work during this time was that of a conscious interjection during a public debate, where a rational and receptive public will recognize the meaning of the provided information and act upon it. Defacements from the Kashmir cluster tended to be text-heavy and multiple paragraphs long. Primary material on the two most active defacer groups in this cluster was available and was used to complete the picture of the defacement scene at this point in time and their motivations. Both groups saw defacements as a way to raise awareness about issues they felt were overlooked in the public debate. Much of the content found in the Kashmir cluster is based on defacers' idea that a rational public sphere would be receptive to the information provided. This shows that defacers at that time were very motivated by geopolitical events and that – at least in the context of the Kashmir conflict – see their role as that of an information provider.

The self-ascribed role of information provider is at odds with the very nature of a web defacement which, by definition overwrites other information. Defacers attempt to mitigate this by defining defacements as a tool of political communication, used mostly because other channels are unavailable for them. This chapter also discussed an inward turn of defacements when, potentially frustrated by a lack of results, defacers stopped attempting to participate in a public discussion through hacked sites and rather turned towards their own community. This frustration can at times be felt in the dataset, and the level of formalization of defacements is high.

What the study of defacements around the Kashmir conflict also found was a dominance of Pakistani voices arguing against Indian politics. Targets were generally divided between Western sites with wider appeals for peace and Indian sites with demands and accusations. When defacers disclosed their nationality or political allegiance, they were operating from a pro-Pakistan or anti-India standpoint. Defacers tried to appeal to different audiences here and as a result had to balance nationalistic appeal aimed at their compatriots, while in relation to a Western audience defacers tended to argue from a pacifist standpoint.

The only voice in this cluster critical of Pakistani involvement in Kashmir is also a defacement indicating the coming change the scene will undergo between Kashmir and 9/11. This new type of defacement operates not through information, but through narratives and frames re-shaping perception of the entire conflict. It thus marks a diversion from defacements as information provision and a move towards attacks on the integrity of a narrative. To recourse to theoretical conceptualizing of hacktivism, the source material of the myth-making process is undermined in a much more effective way than before in this approach.

Disappointment about the lack of public interest in the conflict runs throughout the Kashmir cluster. It is at times palpable how defacers are frustrated with the lack of public interest in their work and are looking for new forms of expression. The change described in the second defacement represents a change towards a more narrative-driven type of defacement. This type will be seen on a larger scale with the 9/11-themed defacements. For the context of being described in Chapter 5, it represents a way out of the frustration stemming from the largely unsuccessful attempt to partake in political debate through information rich defacements.

8.6 9/11 on the Web 1.0

9/11 can in many ways be seen as the acid test for defacements, as a moment that revealed how defacers saw their own identity and how they saw their audience. To understand the significance of this event for defacements, it must be remembered how defacers are actors in an attention economy no matter how much they like to sport an underdog and outlaw image which is all too eagerly reproduced in public images of hackers. September 2001 brought almost total change to this configuration, as the attention economy market was disturbed – naturally the attacks almost completely took up public attention – and changes in anti-terror legislation brought risk of increased criminalization and persecution for web defacers.

The overall answer to this new situation was for defacers to embrace styles and elements which had been existent before but were rather marginal forms. The first one is to shift the focus towards memorial defacements, mourning and remembering the events of 9/11 while expressing sympathy with the US. Here, the defacement plays on its strengths as it appears suddenly and unexpectedly, confronting the viewer once again with the urgency and immediacy of the terrorist attacks. Instead of providing information, this type of defacement primarily deals in narratives and affective frames and moves away from support for whoever is perceived to be the underdog to support for mainstream politics.

A reaction to increased persecution and criminalization of hackers and defacers under the Patriot Act is a recourse to parts of hacker culture as old as 1999 debates about Kevin Mitnick and even the 1986 *Hacker Manifesto*. In both cases, the unusually strict persecution of a curious mind seeking to explore digital opportunities is a key trope. When defacers now argue that they are not cyber-terrorists, they go to great lengths to stress the harmlessness of their actions and condemn violent action in any way. Persecution of hackers, these defacements argue, is merely the result of a misunderstanding of what hackers want to achieve.

These reactions and the very visible public positioning of defacements shows that defacers for the most part see themselves as part of a larger, US-dominated culture of the global North, and that they assume their audience to be part of that same culture. They reveal defacers as rooted in a westernized Internet culture, defending their place in a public sphere which has been shaken up. Neither narrative-led defacements nor reactions to legislative changes are entirely new to web defacements, but 9/11 is when these types can be seen taking over and replacing the information-led types commonly used before September 2001. During this period, defacers are also aligning themselves with the mainstream in contradiction of assumptions about their countercultural role, the history of hacking, and their perceived self-identity. By publicly expressing sympathy and embracing the general Western reaction to 9/11, defacers claim their place within a mourning public. It is striking to see that defacements critical of the US or supportive of the attacks only appear in small numbers in 2011 in reaction to the killing of bin Laden. This might, however, be owed to the scope of this study which only included English defacements.

Defacers as actors in an attention economy was a theme mentioned earlier, as was defacers' general alignment with issues and perspectives of the global North. It is in this context that WikiLeaks presents itself as a problematic object for defacers. WikiLeaks absorbs attention away from web defacements, and through released documents is potentially undermining the mentioned US-dominated culture of the global North. In how defacers engage with WikiLeaks, a lot about their motivation and political attitudes is revealed.

8.7 The attention economy eats its children

Chapter 7 inquires into the relationship between WikiLeaks and web defacements and defacement archives. This chapter is in many ways the culmination of observations and hypothesis about web defacers which have emerged throughout the previous chapters. In the research data set, an ambiguous and distant attitude to WikiLeaks was found both by defacers and the administrators of Zone-H. In my analysis of their relationship, I argue that defacers are in a competitive situation with WikiLeaks as they are both actors in an attention economy. The limited resource of public attention leads to competition, as is seen the defacements of WikiLeaks-domains, because WikiLeaks is seen as drawing attention away from other forms of hacktivism. This finding is indicative of the heterogeneous and diverse hacker scene with many ideas about the role of hacktivism in general and WikiLeaks specifically. It further shows how ideas of unrestricted, free-flowing information clash with the realities of competition in an attention economy. Even when defacers explicitly support WikiLeaks, the desire to overwrite WikiLeaks domains in order to gain exposure is greater than any felt sense of solidarity. Attempts to provide free access to information, be it through WikiLeaks or defacements, are challenged by a competitive scenario where hacking skills determine who gets the largest share of the limited resource of public attention.

Engagement with the complex of WikiLeaks might be fair game within the defacement scene, yet the relationship between WikiLeaks and Zone-H as a cybercrime archive is more ambiguous. Zone-H is referred to 27 times in WikiLeaks documents, all instances using the site to cite web defacements and no instances describing the site as the source of any hacktivist activity. Zone-H issued a number of statements effectively promoting their neutrality and non-involvement as a mere repository of information about hacked websites. This reaction is strange, considering the overall small number of WikiLeaks-related defacements on Zone-H as well as the uncommented presence of much more controversial material in the repository – most of it outside the scope of this study. This reaction, though, bears resemblance to individual efforts to portray defacements as harmless and in no way related to terrorism during the fallout from 9/11. Reasons for this reaction are speculative, yet they are most likely to avoid coming under too much scrutiny as a multiplier of leaked documents.

The WikiLeaks chapter is somewhat of an epilogue to the previous case studies, a moment where a carefully crafted defacer identity and real-life politics intersect and force actors to position themselves. It unravels conflict between the ideological backdrop of web defacements and the conditions of competition for limited resources and it shows the double role of the repository as an information capitalist who claims to have no connection to the information from which the capital is formed – the digital pecunia non olet. What the previous thoughts on the effect of defacement hinted at, and what can be seen in the data derived from the research data set, is a change in trends which occurs around 9/11. In doing so, it shows the value of web archives and studies in web archiving because it is through them it was possible to uncover and describe this junction in the development of online activism. I also propose that in this split, three different pathways for defacements and hacktivism open up. Those defacers who felt dedicated to influencing public debate through information provision have likely taken on a more information capitalist role and might have moved on to projects such as WikiLeaks. Those who saw defacements as tools to manipulate the source material of meaning-making continued to deal in affective frames and narratives, although trends in the platformization of the Internet have led them to expand onto social media. Those who mostly enjoyed defacing pages for the reputation gained within the scene possibly saw little reason to change and continue to hack like it's 1999.

Speaking of effect, the observation made throughout the research data set was that defacers struggled on number of levels such as grammar, rhetoric, web design. That they nevertheless persevered shows the high commitment defacers felt to either their cause, the defacement community, hacking as an informal education or their own curiosity. Defacements are anything but gone, as much as this project largely focussed on 1998-2001 defacements, Zone-H continues to accept submissions and new geopolitical events generate new defacements. Hacktivism and web defacements continue to be actively used practices, testament to their efficiency. However, it is reasonable to assume that at least a part of the defacer community has followed their targets from the homepage of the 2000s Internet to the profile of the web 2.0. With this shift would come new practice and new challenges in the how and what of defacements.

With the developed methodology of this thesis, both technically (how to capture and process these defacements) and structurally (how to describe these strategic interventions into public debate) the future steps are to expand both on the research on the history of political communication online as well as the contemporary relations between digital media and society. First steps have been undertaken to disseminate the methodology through publications and to scale up the scope of the analysed pages.

8.8 Closing thoughts

When planning of this thesis started in late 2016, sourcing of material was not a central concern. I was aware of existing archives and the research done on them and assumed data to be generally available. A quick glance at the structure of the completed work now shows how themes of data availability, metadata, find-ability and preservation run throughout. The research has shown that data on web defacements is anything but widely available – since Samuel's 2014 study of defaced websites, almost all of her sources have gone offline or stopped accepting submissions. Zone-H is now the only known actively collecting archive left. What data was still available suffers from a total lack of metadata describing the content in any way so that now, in the finished thesis, considerable time has been spent locating and retrieving the needles from this enormous haystack. From an academic and archival perspective, there is no collection that would meet the needs of a researcher. While my study also produced a comprehensive capture of material up to the end of 2001, material post-2001 is still very much a terra incognita in terms of defacer groups, topics and styles. This holds great potential for future research, yet is dependent on the continued availability of source material which is far from certain.

As this thesis' web archiving aspect grew throughout the period of research, I became increasingly aware of how fragile and only partially complete these collections are. Finding primary material on some of the most active defacer groups, together with their original home pages, was extraordinarily difficult. It was only through the work of other web archivists that this study was possible and so its mission now is to advocate for the further preservation and academic inclusion of web defacements into digital repositories. There can be speculation about lost material, especially on country-specific collections – and attempts could be made to find and contact owners of now-defunct archives. As this thesis has demonstrated, web defacement archives are valuable cultural documents, not only tracing socio-historical shifts but playing in a part in public meaning-making about those events. To lose material on web defacements is not only to lose parts of web history, it is also to lose cultural and political history.

The contribution of this thesis on one level is the delivery of specific case studies into under-researched online subcultures during specific time periods and in reaction to geopolitical events. Further, the thesis provides a stable and metadata-enriched collection of all political web defacements found in the last remaining community archive from 1999 to 2002. It describes novel ways and challenges when dealing with defaces web pages as a source. Data output follows FAIR principles and has been made available together with all self-developed tools. Through these achievements, the thesis both serves as a starting point for future investigation as well as opens up the entire field of political web defacements to research. Finally, the thesis provides a theoretical understanding that defines hacktivism as interference with the softwareization of society. It frames defaced pages as new sites of subversion brought about by the increased dependence of the medium on its technical infrastructure. This continuous integration opens up a new site of subversion where the defacer may insert their own information into a memory-making process. Through this, the thesis offers a new technocultural toolkit. It understands that computers are more than calculating machines and it speaks and contributes to a shared understanding of computing as a medium of meaningful expression.

Web defacements are not isolated from other forms of online activism. As the platformized web replaced the static home pages of the 2000s, online activism, takeovers and other forms of antagonistic writing transferred with them. The current role of web defacements and the integration of rituals and practices described in this thesis to other platforms are worthwhile future projects which will also depend on robust data collection.

Research ethics in a project that engages with hacked websites will continue to be a complex topic without one definitive solution applicable to all scenarios. Still, it is most important that debates about ethics are had, so that future projects can build on these debates. Hacked websites are, in the context of ethics, two websites combined into one. There is the original page, whose author for the most part is unknown and the content of which is usually completely overwritten by the defacer. Still, through descriptive metadata such as the URL, the original page could be revealed. On top of that lies the defaced page, authored by a more or less known defacer with content potentially featuring identifiable individuals and information. That means that a common scenario in the research of web defacements is two authors, none of which are able to consent to their material being used or presented, at least one set of content (the defaced page) of unclear origin and that content potentially holding information about yet another group. Add to this the fact that political web defacements seldom talk about the weather but human rights violations, war and ongoing conflicts.

General approaches to the complex topic of ethics were borrowed from wider fields of research on archived, old and abandoned web pages. On the level of the original page, it is safe to assume that website owners did not consent to the hacking of their online presence. On the level of the defacers, it is reasonable to assume that by submitting their work to an archive, they also consented to its preservation at the time. These two really different starting points must be considered in the research design. This includes minimizing data where consent cannot be assumed. As for the original pages, no URLs were given that would expose an individual person, such as www.michaelkurzmeier.com. Most defacements do not refer to the original page in a relevant way or at all, so that usually the TLD (.com in the above example) was enough to situate the original in relation to the defaced page.

As for the defacers, the research design was such that is focussed on their online presence and persona. Whatever nickname their used for themselves in logos, interviews and on their own home pages was used throughout the analysis with no intention of exposing the real-life person behind the alias. It is important to keep in mind that this study investigates web defacements for their form and content, and not as traces of a defacer’s physical identity.

With the change from an informational to a narrative style in defacements identified in this analysis, more information about individuals is found on a content level. Additionally, with a change in web design over time, more visual material is being used. While a reverse image search in most cases reveals that defacers tend to reuse press photos, it was nevertheless decided to blur out faces. That said, the amount of problematic content, such as content directed at exposing one individual was much lower than expected. This was potentially due to the scope being set as defacements engaged with political content. Still, ethics remain a complex topic to which there can be no one definitive answer. The approach of understanding the different perspectives coming together in defacements and the principle of data minimization has proven itself throughout this study. Because of this complexity, it is vital that any future research in this area adequately explore and have broad conversations about the ethical frameworks of this kind of data collection and analysis.

What remains is the question of the effect and legacy of web defacements. Throughout this thesis, in the case study examples and in the surviving primary materials, the tremendous effort with which defacers, hackers and cyber security enthusiasts have either created defacements or created the infrastructure around them has been shown. It has also been shown how defacements fluctuate between communicating to an audience outside the scene and communicating to a scene-internal audience. The research has shown that defacements can fulfil both functions, yet what is implied is that defacements might be formalized pieces of expression aimed at a small group of insiders rather than injections into public discourse.

The material presented in this thesis, as interesting and insightful as it is, is but a fraction of the tip of the iceberg. Through an advocacy for the use of defacements to enhance the understanding not only of a single website's history, but for the research of social movements and political expression online, this thesis has continuously emphasized the need for stable, usable and reliable archives of defaced websites. The research methodology presented as well as the knowledge and skills obtained over the years of developing and conducting this research can serve as the first steps towards that goal.

9. Bibliography

Abela, Robert. 2020. ‘Statistics Show Why WordPress Is a Popular Hacker Target’. WP White Security. 25 June 2020. https://www.wpwhitesecurity.com/statistics-70-percent-wordpress-installations-vulnerable/.

AIC. n.d. ‘About Us’. Accessed 6 May 2020. https://web.archive.org/save/http://www.lordpimp.20m.com/AIC/Main.htm.

Akhtar, Rais, and William Kirk. 2019. ‘Jammu and Kashmir’. In *Encyclopædia Britannica*. https://www.britannica.com/place/Jammu-and-Kashmir.

Alexander, Katharine, and Rachel Alexander. 2018. ‘European Commission Communication on Tackling Illegal Content Online: Towards an Enhanced Responsibility of Online Platforms’. *Entertainment Law Review* 29 (2).

Almeida, Marcelo. 2008. ‘Statistics Report 2005-2007’. 3 April 2008. http://www.zone-h.org/news/id/4686.

Andrejevic, Mark. 2013. *InfoGlut.* London: Taylor & Francis.

Antracoli, Alexis, Steven Duckworth, Judith Silva, and Kristen Yarmey. 2014. ‘Capture All the URLs: First Steps in Web Archiving’. *Pennsylvania Libraries: Research & Practice* 2 (2): 155–70. https://doi.org/10.5195/PALRAP.2014.67.

Attrition.org. n.d. ‘Attrition - about Us’. Attrition.Org. Accessed 15 February 2019. http://attrition.org/attrition/.

Atwan, Abdel Bari. 2015. *Islamic State: The Digital Caliphate*. Oakland, California: University of California Press.

Ayiter, Elif. n.d. ‘Telling Tales in Smooth and Striated Spaces’. Sabancı University. Accessed 11 March 2020. http://research.sabanciuniv.edu/33617/1/ayiter_telling-tales-in-smooth-striated.pdf.

Baldick, Chris. 2004. *The Concise Oxford Dictionary of Literary Terms*. 2nd ed. Oxford Paperback Reference. Oxford ; New York: Oxford University Press.

Balduzzi, Marco, Ryan Flores, Lion Gu, and Federico Maggi. 2018. ‘A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks’. Trend Micro Forward-Looking Threat Research (FTR) Team.

Ball, Alex. 2010. ‘DCC State of the Art Report: Web Archiving’. University of Edinburgh; UKOLN, University of Bath; HATII, University of Glasgow; Science and Technology Facilities Council, 2010. Edinburgh Research Archive (era). http://hdl.handle.net/1842/3327.

Barlow, John Perry. 1996. ‘A Declaration of the Independence of Cyberspace’. https://www.eff.org/cyberspace-independence.

Barnes, Elizabeth. 1997. *‘Politics of Sympathy.’ States of Sympathy: Seduction and Democracy in the American Novel*. New York: Columbia University Press.

Barthes, Roland, and Stephen Heath. 1987. *Image, Music, Text*. London: Fontana Press.

Barthes, Roland, and Annette Lavers. 2006. *Mythologies*. 47. [print.]. New York, NY: Hill and Wang.

Bawcutt, P. 2015. ‘The Source and Significance of a Marginal Inscription in the Buik of Alexander (c.1580)’. *Notes and Queries* 62 (1): 56–58. https://doi.org/10.1093/notesj/gju226.

Baym, Nancy K. 2010. *Personal Connections in the Digital Age*. Cambridge, UK ; Malden, MA: Polity.

Bechmann, Anja, Michael Zimmer, Charles M. Ess, and Aline Shakti Franze. 2020. ‘Internet Research: Ethical Guidelines 3.0’. Association of Internet Researchers. https://aoir.org/reports/ethics3.pdf.

Beller, Jonathan. 2006. *The Cinematic Mode of Production Attention Economy and the Society of the Spectacle*. Hanover, N.H.: Dartmouth College Press : University Press of New England.

Ben-David, Anat. 2020. ‘Counter-Archiving Facebook’. *European Journal of Communication*, May, 026732312092206. https://doi.org/10.1177/0267323120922069.

Berry, David M. 2008. *Copy, Rip, Burn: The Politics of Copyleft and Open Source*. London: Pluto Press.

———. 2014. *Critical Theory and the Digital*. Critical Theory and Contemporary Society. New York: Bloomsbury.

Bhat, Sabzar Ahmad. 2019. ‘The Kashmir Conflict and Human Rights’. *Race & Class* 61 (1): 77–86. https://doi.org/10.1177/0306396819850988.

Bird, Steven, Ewan Klein, and Edward Loper. 2009. *Natural Language Processing with Python*. O’Reilly Media Inc. http://www.nltk.org/book/.

Blom, Ina, Trond Lundemo, and Eivind Røssaak, eds. 2017. *Memory in Motion: Archives, Technology, and the Social*. Recursions: Theories of Media, Materiality, and Cultural Techniques. Amsterdam: Amsterdam University Press.

Bragg, Molly, and Hanna Kristine. 2013. ‘The Web Archiving Life Cycle Model’. The Archive-It Team, Internet Archive. https://archive-it.org/static/files/archiveit_life_cycle_model.pdf.

Brügger, Niels. 2005. *Archiving Websites: General Considerations and Strategies*. Århus, Denmark: Centre for Internet Research.

———. 2018. *The Archived Web: Doing History in the Digital Age*. Cambridge, Massachusetts: The MIT Press.

Bunt, Gary R. 2003. *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments*. London; Sterling, Va.: Pluto Press.

Burstein, Andrew. 1999. *Sentimental Democracy: The Evolution of America’s Romantic Self-Image*. New York: Hill and Wang.

Cacciatore, Michael A., Dietram A. Scheufele, and Shanto Iyengar. 2016. ‘The End of Framing as We Know It … and the Future of Media Effects’. *Mass Communication and Society* 19 (1): 7–23. https://doi.org/10.1080/15205436.2015.1068811.

Calhoun, Craig. 2004. ‘Information Technology and the International Public Sphere’. In *Shaping the Network Society: The New Role of Civil Society in Cyberspace*, 229–52. Cambridge, MA: MIT Press.

———. 2010. ‘The Public Sphere in the Field of Power’. *Social Science History* 34 (3): 301–35. https://doi.org/10.1215/01455532-2010-003.

Cammaerts, Bart. 2013. ‘Networked Resistance: The Case of WikiLeaks’. *Journal of Computer-Mediated Communication* 18 (4): 420–36. https://doi.org/10.1111/jcc4.12024.

Carnegie Mellon University CyLab. 2017. ‘The ReCAPTCHA Project’. 27 October 2017. https://web.archive.org/web/20171027203659/https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html.

Castells, Manuel. 2009. *Communication Power*. Oxford ; New York: Oxford University Press.

———. 2010. *The Rise of the Network Society*. 2nd ed., with A new pref. The Information Age : Economy, Society, and Culture, v. 1. Chichester, West Sussex ; Malden, MA: Wiley-Blackwell.

———. 2013. *Communication Power*. 2nd edition. Oxford: Oxford University Press.

Chandler, Daniel, and Rod Munday. 2016. ‘Walled Garden’. In *A Dictionary of Social Media*. Oxford University Press. http://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093.

Christensen, Christian. 2014a. ‘WikiLeaks and the Afterlife of Collateral Murder.’ *International Journal of Communication (19328036)* 8 (January): 2593–2602.

———. 2014b. ‘A Decade of WikiLeaks: So What?’ *International Journal of Media & Cultural Politics* 10 (3): 273–84. https://doi.org/10.1386/macp.10.3.273_1.

Clarke, Roger. 2004. ‘Information Wants to Be Free ...’ 24 February 2004. http://www.rogerclarke.com/II/IWtbF.html.

Coleman, E. Gabriella. 2013. ‘Anonymous in Context: The Politics and Power behind the Mask’. *Internet Governance Papers*, September 2013. https://www.cigionline.org/sites/default/files/no3_8.pdf.

———. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London ; New York: Verso.

Coyle, Diane. 2017. ‘Precarious and Productive Work in the Digital Economy’. *National Institute Economic Review* 240 (1): R5–14. https://doi.org/10.1177/002795011724000110.

Crawford, Neta C., and Catherine Lutz. 2021. ‘Human Cost of Post-9/11 Wars: Direct War Deaths in Major War Zones, Afghanistan & Pakistan (Oct. 2001 – Aug. 2021); Iraq (March 2003 – Aug. 2021); Syria (Sept. 2014 – May 2021); Yemen (Oct. 2002-Aug. 2021) and Other Post-9/11 War Zones’. Brown University. https://watson.brown.edu/costsofwar/files/cow/imce/papers/2021/Costs%20of%20War_Direct%20War%20Deaths_9.1.21.pdf.

Curtis, Adam. 2016. *Hypernormalization*. BBC. https://www.bbc.co.uk/iplayer/episode/p04b183c/adam-curtis-hypernormalisation.

Dahlgren, Peter. 2013. *The Political Web: Media, Participation and Alternative Democracy*. Basingstoke, Hampshire: Palgrave Macmillan.

D’Angelo, Paul, and Jim A Kuypers. 2010. *Doing News Framing Analysis: Empirical and Theoretical Perspectives*. New York: Routledge.

Davies, L., and E. Razlogova. 2013. ‘Framing the Contested History of Digital Culture’. *Radical History Review* 2013 (117): 5–31. https://doi.org/10.1215/01636545-2210446.

Davis, Amanda. 2015. ‘A History of Hacking’. *IEEE - The Institute*, March. http://theinstitute.ieee.org/technology-topics/cybersecurity/a-history-of-hacking.

Debord, Guy. 1994. *The Society of the Spectacle*. New York: Zone Books.

Deleuze, Gilles, and Félix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press.

Denning, Dorothe E. 1999. ‘Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy’. *Global Problem Solving Information Technology and Tools*, December. https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/.

Derrida, Jacques. 1996. *Archive Fever : A Freudian Impression*. Religion and Postmodernism. Chicago: University of Chicago Press.

Deseriis, Marco. 2017. ‘Hacktivism: On the Use of Botnets in Cyberattacks’. *Theory, Culture & Society* 34 (4): 131–52. https://doi.org/10.1177/0263276416667198.

Dobson, Kathy, and Jeremy Hunsinger. 2016. ‘The Political Economy of WikiLeaks: Transparency and Accountability through Digital and Alternative Media’. *Interactions: Studies in Communication & Culture* 7 (2): 217–33. https://doi.org/10.1386/iscc.7.2.217_1.

Dormon, Bob. 2016. ‘How the Internet Works: Submarine Fiber, Brains in Jars, and Coaxial Cables’. Ars Technica. 26 May 2016. https://arstechnica.com/information-technology/2016/05/how-the-internet-works-submarine-cables-data-centres-last-mile/2/.

Douglas, Ann. 1988. *The Feminization of American Culture*. The Anchor Library of Sociology. New York: Anchor Press/Doubleday.

Eco, Umberto. 1984. *Semiotics and the Philosophy of Language*. London: Macmillan.

Electronic Frontier Foundation. n.d. ‘A History of Protecting Freedom Where Law and Technology Collide’. Accessed 9 August 2021. https://www.eff.org/about/history.

Erdogan, Erdogan. 2020. ‘West and East German Hackers from a Comparative Perspective’’. *Widescreen* 23. http://widerscreen.fi/numerot/2020-2-3/west-and-east-german-hackers-from-a-comparative-perspective/.

Erll, Astrid, and Ann Rigney. 2009. ‘Cultural Memory and Its Dynamics’. In *Mediation, Remediation, and the Dynamics of Cultural Memory*, 1–14. Media and Cultural Memory = Medien Und Kulturelle Erinnerung 10. Berlin ; New York: Walter de Gruyter.

Ernst, Wolfgang, and Jussi Parikka. 2013. *Digital Memory and the Archive*. Minneapolis, MN: University of Minnesota Press.

Fernandez, Kevin. 2012. ‘Zone-H Celebrates Its 10 Years!’ Zone-H. 3 September 2012. https://www.zone-h.org/news/id/4742.

Ferrell, Henry. 2017. ‘Hackers Have Just Dumped a Treasure Trove of NSA Data. Here’s What It Means.’ *The Washington Post*, 15 April 2017. https://web.archive.org/save/https://www.washingtonpost.com/news/monkey-cage/wp/2017/04/15/shadowy-hackers-have-just-dumped-a-treasure-trove-of-nsa-data-heres-what-it-means/. https://www.washingtonpost.com/news/monkey-cage/wp/2017/04/15/shad owy-hackers-have-just-dumped-a-treasure-trove-of-nsa-data-heres-what-it-means/.

Free Software Foundation. 2021. ‘What Is Free Software?’ https://web.archive.org/web/20210427085316/https://www.gnu.org/philosophy/free-sw.html#f1. https://www.gnu.org/philosophy/free-sw.html#f1.

Fuchs, Christian. 2014. ‘Anonymous: Hacktivism and Contemporary Politics’. In *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*, edited by Daniel Trottier and Christian Fuchs, 88–108. Routledge Research in Information Technology and Society 16. New York: Routledge.

Fuller, Steve. 2018. *Post-Truth: Knowledge as a Power Game*. Anthem’s Key Issues in Modern Sociology. New York: Anthem Press.

Galloway, Alexander. 2006. *Protocol: How Control Exists after Decentralization*. Leonardo. Cambridge, Mass.: MIT Press.

———. 2015. ‘Black Box Architecture’. *Culture and Communication* (blog). 13 January 2015. http://cultureandcommunication.org/galloway/black-box-architecture.

Galloway, Alexander, and Eugene Thacker. 2007. *The Exploit : A Theory of Networks*. Electronic Mediations 21. Minneapolis: University of Minnesota Press.

GForce Pakistan. 2000. HWA-Security Interview Interview by SugarKing. https://web.archive.org/web/20010813213544/http://www.hwa-security.net/gforce.txt.

———. n.d. Arab Magazine Interview Interview by Fadi Salem. Accessed 6 May 2020a. https://web.archive.org/web/20010813174748/http://gforcep.addr.com/arab.txt.

———. n.d. India Cracked Interview with GForce Pakistan Interview by Srijith Nair. Accessed 6 May 2020b. https://web.archive.org/web/20040616082021/http://www.srijith.net/indiacracked/interviews/gforce.shtml.

Gillespie, Tarleton. 2010. ‘The Politics of “Platforms”’. *New Media & Society* 12 (3): 347–64. https://doi.org/10.1177/1461444809342738.

Goodman, Seymour E. 1979. ‘Soviet Computing and Technology Transfer: An Overview’. *World Politics* 31 (4): 539–70. https://doi.org/10.2307/2009909.

Grabbe. 2016. ‘Word Frequency Effects for LEET Lettering in Word Recognition’. *The American Journal of Psychology* 129 (1): 37. https://doi.org/10.5406/amerjpsyc.129.1.0037.

Graham, Mark, Isis Hjorth, and Vili Lehdonvirta. 2017. ‘Digital Labour and Development: Impacts of Global Digital Labour Platforms and the Gig Economy on Worker Livelihoods’. *Transfer: European Review of Labour and Research* 23 (2): 135–62. https://doi.org/10.1177/1024258916687250.

Gul, Sumeer, Tariq Ahmad Shah, and Suhail Ahmad. 2014. ‘Digital User Behaviour of Academicians in a Conflict Zone, Kashmir: Comparing Log Analysis of Electronic Resources in the Times of Conflict and Peace’. *Program* 48 (2): 127–39. https://doi.org/10.1108/PROG-06-2013-0026.

Habermas, Jürgen. 1976. *Technik Und Wissenschaft Als ‘Ideologie’*. 8. Aufl. Edition Suhrkamp 287. Frankfurt am Main: Suhrkamp.

———. 1984. *The Theory of Communicative Action*. Boston: Beacon Press.

———. 1989. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Studies in Contemporary German Social Thought. Cambridge, Mass: MIT Press.

Habermas, Jürgen, and Maeve Cooke. 1998. *On the Pragmatics of Communication*. Studies in Contemporary German Social Thought. Cambridge, Mass: MIT Press.

'Hack'. n.d. In *Merriam-Webster.Com Dictionary*. https://www.merriam-webster.com/dictionary/hack.

Hansen, Anders, and David Machin. 2013. *Media and Communication Research Methods*. Basingstoke, Hampshire: Palgrave Macmillan.

Healy, Sharon. 2017. 'The Web Archiving of Irish Election Campaigns: A Case Study into the Usefulness of the Irish Web Archive for Researchers and Historians'. In . University of London. http://netpreserve.org/wac2017/abstracts/#_abstract74.

Herman, Edward S., and Noam Chomsky. 1988. *Manufacturing Consent: The Political Economy of the Mass Media*. 1st ed. New York: Pantheon Books.

Higa, Darold. 2008. 'Walled Gardens versus the Wild West'. *Computer* 41 (10): 102–5. https://doi.org/10.1109/MC.2008.439.

Himanen, Pekka. 2001. *The Hacker Ethic: And the Spirit of the Information Age*. London: Secker & Warburg.

Hoeren, T. 2009. 'The European Liability and Responsibility of Providers of Online-Platforms Such as "Second Life"'. *Journal of Information, Law & Technology (JILT),* no. 1/2009 (May). http://go.warwick.ac.uk/jilt/2009_1/hoeren.

Hofmann, Markus, and Andrew Chisholm, eds. 2016. *Text Mining and Visualization: Case Studies Using Open-Source Tools*. Chapman & Hall/CRC Data Mining and Knowledge Discovery Series. Boca Raton: CRC Press.

Holwerda, Tom. 2000. 'Mosaic - The First Global Web Browser'. 7 January 2000. https://www.livinginternet.com/w/wi_mosaic.htm.

Hopkins, Todd. 2014. 'Virtual Graffiti: Dyscribing Humans'. Ottawa, Canada: Carleton University. https://web.archive.org/web/20200604025024/https://curve.carleton.ca/system/files/etd/9ef84295-5316-4532-a776-8ceeecb3fcfa/etd_pdf/db2d82e78e60f268c42e29641109eeed/hopkins-virtualgraffitidyscribinghumans.pdf. https://curve.carleton.ca/system/files/etd/9ef84295-5316-4532-a776-8ceeecb3fcfa/etd_pdf/db2d82e78e60f268c42e29641109eeed/hopkins-virtualgraffitidyscribinghumans.pdf.

Hoskins, Andrew. 2009. 'Digital Network Memory'. In *Mediation, Remediation, and the Dynamics of Cultural Memory*. Berlin; New York: W. de Gruyter.

ISC. 2008. 'Top Level Domains By Host Count'. https://ftp.isc.org/www/survey/reports/current/bynum.txt.

Jackson, H. J. 2001. *Marginalia: Readers Writing in Books*. New Haven: Yale University Press.

Jarvis, Lee. 2011. '9/11 Digitally Remastered? Internet Archives, Vernacular Memories and WhereWereYou.Org'. *Journal of American Studies* 45 (4): 793–814. https://doi.org/10.1017/S002187581100096X.

Jordan, Tim. 2002. *Activism! Direct Action, Hacktivism and the Future of Society*. Focus on Contemporary Issues. London: Reaktion Books.

———. 2015. *Information Politics: Liberation and Exploitation in the Digital Society*. Digital Barricades : Interventions in Digital Culture and Politics. London: Pluto Press.

Jordan, Tim, and Paul A. Taylor. 2004. *Hacktivism and Cyberwars: Rebels with a Cause?* 1st ed. London: Routledge.

Karhula, Päivikki. 2012. ‘What Is the Effect of WikiLeaks for Freedom of Information?’ International Federation of Library Associations and Institutions. https://web.archive.org/web/20120630172755/http://www.ifla.org/publications/what-is-the-effect-of-wikileaks-for-freedom-of-information. https://www.ifla.org/files/assets/faife/publications/spotlights/wikileaks-karhula.pdf.

Kelly, Jamie Terence. 2012. *Framing Democracy A Behavioral Approach to Democratic Theory*.

Kennedy, Helen, Rosemary Lucy Hill, William Allen, and Andy Kirk. 2016. ‘Engaging with (Big) Data Visualizations: Factors That Affect Engagement and Resulting New Definitions of Effectiveness’. *First Monday*, November. https://doi.org/10.5210/fm.v21i11.6389.

Kerr, Paul K., Catharine A. Theohary, and John Rollins. 2010. ‘The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability’. 7–5700. Congressional Research Service. https://fas.org/sgp/crs/natsec/R41524.pdf.

Kete, Mary Louise. 2000. *Sentimental Collaborations: Mourning and Middle-Class Identity in Nineteenth Century America*. Durham, NC. [u.a.]: Duke Univ. Press.

Kirschenbaum, Matthew G. 2012. *Mechanisms: New Media and the Forensic Imagination*. 1. paperback ed. Cambridge, Mass: MIT Press.

Kübler-Ross, Elisabeth. 1997. *On Death and Dying*. New York: Schribner.

Kurzmeier, Michael. 2020. ‘Towards a Concept for Archiving Hacked Websites’. *NPPSH Reflections* 3: 35–58.

Lapsley, Phil, and Steve Wozniak. 2013. *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*.

Lasn, Kalle. 2000. *Culture Jam: How to Reverse Americans’ Suicidal Consumer Binge - and Why We Must*. 1. Quill ed. New York: Quill.

Lessig, Lawrence. 2006. *Code*. Version 2.0. New York: Basic Books.

Lialina, Olia. 2005. ‘A Vernacular Web. The Indigenous and The Barbarians’. January 2005. http://art.teleportacia.org/observation/vernacular/.

Licklider, J.C.R. 1960. ‘Man-Computer Symbiosis’. *IRE Transactions on Human Factors in Electronics* HFE-1 (March): 4–11.

Lievrouw, Leah A. 2011. *Alternative and Activist New Media*. Digital Media and Society Series. Cambridge, UK ; Malden, MA: Polity.

Lin, Patrick. 2016. *Ethics of Hacking Back*. San Luis Obispo, California: California Polytechnic State UniversityEthics + Emerging Sciences Group. http://ethics.calpoly.edu/hackingback.pdf.

Lingel, Jessica. 2017. *Digital Countercultures and the Struggle for Community*. The Information Society Series. Cambridge, MA: The MIT Press.

‘Linux Logos and Mascots’. n.d. Linux.Org. Accessed 9 March 2020. https://web.archive.org/web/20040401161253/http://www.linux.org/info/logos.html.

Lloyd, William Forster. 1833. *Two Lectures on the Checks to Population*. Oxford; London: University of Oxford.

Lomborg, Stine. 2018. ‘Ethical Considerations for Web Archives and Web History Research’. In *The Sage Handbook of Web History*, edited by Niels Brügger and Ian Miligan, 99–111. Thousand Oaks, CA: SAGE Inc.

Lyons, Martyn. 2011. *Books: A Living History*. Los Angeles: J. Paul Getty Museum.

Maggi, Federico, Marco Balduzzi, Ryan Flores, Lion Gu, and Vincenzo Ciancaglini. 2018. ‘Investigating Web Defacement Campaigns at Large’. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security - ASIACCS ’18*, 443–56. Incheon, Republic of Korea: ACM Press. https://doi.org/10.1145/3196494.3196542.

Manning, Christopher D., Prabhakar Raghavan, and Hinrich Schütze. 2008. *Introduction to Information Retrieval*. New York: Cambridge University Press.

Marks, Paul. 2011. ‘Dot-Dash-Diss: The Gentleman Hacker’s 1903 Lulz’, December. https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/#.VN0Z-0tmmJc.

Matic, Veran. 2004. ‘Civil Networking in a Hostile Environment: Experiences in the Former Yugoslavia’. In *Shaping the Network Society: The New Role of Civil Society in Cyberspace*, 159–85. Cambridge, Mass: MIT Press.

Maynooth University Research Ethics Policy and Committee. 2016. ‘Maynooth University Research Ethics Policy’. https://www.maynoothuniversity.ie/sites/default/files/assets/document/Maynooth%20University%20Research%20Ethics%20Policy%20June%202016_0.pdf.

McDonald, Kevin. 2015. ‘From Indymedia to Anonymous: Rethinking Action and Identity in Digital Cultures’. *Information, Communication & Society* 18 (8): 968–82. https://doi.org/10.1080/1369118X.2015.1039561.

McLuhan, Marshall. 1962. *The Gutenberg Galaxy: The Making of Typographic Man*. London: Routledge & Kegan Paul.

Merrell, Floyd. 2016. *Peirce, Signs, and Meaning*.

Miligan, Ian. 2018. ‘Ethics and the Archived Web Presentation: “The Ethics of Studying GeoCities”’. *Digital History, Web Archiving, and Contemporary History* (blog). 27 March 2018. https://ianmilligan.ca/2018/03/27/ethics-and-the-archived-web-presentation-the-ethics-of-studying-geocities/.

Milone, Mark G. 2002. ‘Hacktivism: Securing the National Infrastructure’. *The Business Lawyer* 58 (1): 383–413.

Minor. 2010. ‘Notes on the Wikileaks Case’. Zone-H. 12 October 2010. http://www.zone-h.org/news/id/4736.

Mitnick, Kevin D., and William L. Simon. 2005. *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders, & Deceivers*. Indianapolis, IN: Wiley.

———. 2011. *Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker*. 1st ed. New York: Little, Brown and Company.

Moulthrop, Stuart, and Dene Grigar. 2015. ‘Pathfinders : Documenting the Experience of Early Digital Literature’. https://doi.org/10.7273/WF0B-TQ14.

Musiani, Francesca. 2011. ‘Privacy as Invisibility: Pervasive Surveillance and the Privatization of Peer-to-Peer Systems’. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable*

Information Society 9 (2): 126–40. https://doi.org/10.31269/triplec.v9i2.248.

Nagle, Angela. 2017. *Kill All Normies: The Online Culture Wars from Tumblr and 4chan to the Alt-Right and Trump*. Winchester, UK ; Washington, USA: Zero Books.

National Commission on Terrorist Attacks Upon the United States. 2004. ‘The 9/11 Commission Report’. https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf.

National Infrastructure Protection Center. 2001. ‘Cyber Protests: The Threat to the U.S. Information Infrastructure’. National Infrastructure Protection Center. http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.pdf.

National Science Foundation. 2003. ‘A Brief History of NSF and the Internet’. https://web.archive.org/save/https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050. https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

Naughton, John. 2001. *A Brief History of the Future: The Origins of the Internet*. 4. impr. London: Phoenix.

Nelson, Theodor H. 1983. *Computer Lib*. 9. print. South Bend, Ind: The Distributors.

Network Working Group. 1989. ‘Request for Comments 1122’. Internet Engeneering Task force. https://tools.ietf.org/pdf/rfc1122.pdf.

Norris, Pippa, Montague Kern, and Marion R. Just, eds. 2003. *Framing Terrorism: The News Media, the Government, and the Public*. New York: Routledge.

Odell, Jenny. 2019. *How to Do Nothing: Resisting the Attention Economy*. Brooklyn, NY: Melville House.

Ogden, Charles K., and Ivor A. Richards. 1985. *The Meaning of Meaning: A Study of the Influence of Language upon Thought and the Science of Symbolism*. London: Ark Paperbacks.

Paganoni, Maria Cristina. 2011. ‘Blogging 9/11 and Memory Discourse’. *Altre Modernità*, September, 279-294 Pages. https://doi.org/10.13130/2035-7680/1309.

Palmer, Denny. 2021. ‘What Is Ransomware? Everything You Need to Know about One of the Biggest Menaces on the Web’. *ZDNet*, 10 May 2021. https://web.archive.org/web/20210908082933/https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/. https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/.

Papacharissi, Zizi. 2010. *A Private Sphere: Democracy in a Digital Age*. Digital Media and Society. Cambridge, UK ; Malden, MA: Polity.

———. 2016. ‘Affective Publics and Structures of Storytelling: Sentiment, Events and Mediality’. *Information, Communication & Society* 19 (3): 307–24. https://doi.org/10.1080/1369118X.2015.1109697.

Parashar, Swati. 2018. ‘Competing Masculinities, Militarization and the Conflict in Kashmir’. *International Feminist Journal of Politics* 20 (4): 663–65. https://doi.org/10.1080/14616742.2018.1532179.

Parikka, Jussi. 2015. *A Geology of Media*. Electronic Mediations, volume 46. Minneapolis ; London: University of Minnesota Press.

Pedersen, Peter Ole. 2013. ‘The Never-Ending Disaster: 9/11 Conspiracy Theory and the Integration of Activist Documentary on Video Websites’. *Acta*

Universitatis Sapientiae, Film and Media Studies 6 (1): 49–64. https://doi.org/10.2478/ausfm-2014-0004.

Perkins, Jacob. 2010. *Python Text Processing with NLTK 2.0 Cookbook: Over 80 Practical Recipes for Using Python's NLTK Suite of Libraries to Maximize Your Natural Language Processing Capabilities ; [Quick Answeers to Common Problems]*. Quick Answers to Common Problems. Birmingham: Packt Publ.

Petrick, Elizabeth. 2017. 'Imagining the Personal Computer: Conceptualizations of the Homebrew Computer Club 1975–1977'. *IEEE Annals of the History of Computing* 39 (4): 27–39. https://doi.org/10.1109/MAHC.2018.1221045.

Poell, Thomas. 2014. 'Social Media Activism and State Censorship'. In *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*, edited by Daniel Trottier and Christian Fuchs, 189–208. Routledge Research in Information Technology and Society 16. New York: Routledge.

Poor, Nathaniel, and Roei Davidson. 2016. 'The Ethics of Using Hacked Data:Patreon's Data Hack and Academic Data Standards'. Data&Society. https://web.archive.org/web/20200107135548/https://bdes.datasociety.net/wp-content/uploads/2016/10/Patreon-Case-Study.pdf. https://bdes.datasociety.net/wp-content/uploads/2016/10/Patreon-Case-Study.pdf.

Postel, J. 1994. 'RFC1591'. IETF. https://tools.ietf.org/html/rfc1591.

Preatoni, Roberto. 2009. 'E2-Labs' Project Ethan Dissected. Anatomy of a Franchise Proposal Based on Non-Existing Partnerships (UPDATED)'. Zone-H. 22 November 2009. https://www.zone-h.org/news/id/4731.

Raymond, Eric S. 2001. *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Rev. ed. Beijing ; Cambridge, Mass: O'Reilly.

Rheingold, Howard. 2000a. *The Virtual Community: Homesteading on the Electronic Frontier*. Rev. ed. Cambridge, Mass: MIT Press.

———. 2000b. *Tools for Thought: The History and Future of Mind-Expanding Technology*. 1st MIT Press ed. Cambridge, Mass: MIT Press.

———. 2002. *Smart Mobs: The next Social Revolution*. Cambridge, MA: Perseus Pub.

Richterich, Annika. 2018. 'Tracing Controversies in Hacker Communities: Ethical Considerations for Internet Research'. *Information, Communication & Society*, July, 1–18. https://doi.org/10.1080/1369118X.2018.1486867.

Robins, Kevin, and Frank Webster. 1998. 'Cybernetic Capitalism, Informationalism and Cognitive Labor'. In *The Political Economy of Information*, 44–75. University of Wisconsin Press.

Rogers, APV, and Dominic McGoldrick. 2011. 'Assassination and Targeted Killing—the Killing of Osama Bin Laden'. *The International and Comparative Law Quarterly* 60 (3): 778–88.

Rogers, Richard. 2013. *Digital Methods*. Cambridge, Massachusetts: The MIT Press.

Romagna, Marco, and Niek Jan van den Hout. 2017. 'Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats'. In .

Roosewelt, Franklin D. 1941. ‘1941 State of the Union Address “the Four Freedoms”’. https://voicesofdemocracy.umd.edu/fdr-the-four-freedoms-speech-text/.

Salem, Sarah. 2014. ‘Creating Spaces for Dissent. The Role of Social Media in the 2011 Egyptian Revolution’. In *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*, edited by Daniel Trottier and Christian Fuchs, 171–88. Routledge Research in Information Technology and Society 16. New York: Routledge.

Samuel, Alexandra. 2014. ‘Hacktivism and the Future of Political Participation’. Cambridge, Massachusetts: Harvard University. http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.

Saussure, Ferdinand de, Charles Bally, and Wade Baskin. 1966. *Course in General Linguistics*. 1st paperback ed. MacGraw-Hill Paperbacks. New York, NY: McGraw-Hill.

Schmitt, Xavier, Sylvain Kubler, Jeremy Robert, Mike Papadakis, and Yves LeTraon. 2019. ‘A Replicable Comparison Study of NER Software: StanfordNLP, NLTK, OpenNLP, SpaCy, Gate’. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, 338–43. Granada, Spain: IEEE. https://doi.org/10.1109/SNAMS.2019.8931850.

Schofield, Tom, David Kirk, and Mitchell Whitelaw. 2017. ‘Research through Design and Digital Humanities in Practice: What, How and Who in an Archive Research Project’. *Digital Scholarship in the Humanities* 32 (suppl_1): i103–20. https://doi.org/10.1093/llc/fqx005.

Schofield, Victoria. 2010. *Kashmir in Conflict: India, Pakistan and the Unending War*. Fully revised ed. London: Tauris.

Sciberras, Nicohlas. 2019. ‘Configuring Your Web Server to Not Disclose Its Identity’. The Acutenix Blog. 15 May 2019. https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/.

‘Script Kiddy’. 2018. In *Technopedia*. https://www.techopedia.com/definition/4090/script-kiddie.

SilentStorm. 2002. Interview : SilentStorm of Brazil Hackers SabotageZataz. https://web.archive.org/web/20021128202158/http://www.zataz.com/zataz v7/bhs1.htm.

Söderberg, Johan. 2008. *Hacking Capitalism: The Free and Open Source Software Movement*. 270 Madison Ave, New York, NY 10016: Routledge.

Spence, Alexa, and Nick Pidgeon. 2010. ‘Framing and Communicating Climate Change: The Effects of Distance and Outcome Frame Manipulations’. *Global Environmental Change* 20 (4): 656–67. https://doi.org/10.1016/j.gloenvcha.2010.07.002.

Sreelakshmi, K, B Premjith, and K.P. Soman. 2020. ‘Detection of Hate Speech Text in Hindi-English Code-Mixed Data’. *Procedia Computer Science* 171: 737–44. https://doi.org/10.1016/j.procs.2020.04.080.

Stallman, Richard M. 2009. ‘Why “Open Source” Misses the Point of Free Software’. *Communications of the ACM* 52 (6): 31. https://doi.org/10.1145/1516046.1516058.

Stallman, Richard M., and Joshua Gay. 2002. *Free Software, Free Society: Selected Essays*. 1st. ed. Boston, Mass: Free Software Foundation.

Stempel, Carl, Thomas Hargrove, and Guido H. Stempel. 2007. ‘Media Use, Social Structure, and Belief in 9/11 Conspiracy Theories’. *Journalism & Mass Communication Quarterly* 84 (2): 353–72. https://doi.org/10.1177/107769900708400210.

Streeb, Dirk, Mennatallah El-Assady, Daniel Keim, and Min Chen. 2019. ‘Why Visualize? Untangling a Large Network of Arguments’. *IEEE Transactions on Visualization and Computer Graphics*, 1–1. https://doi.org/10.1109/TVCG.2019.2940026.

Streeter, Thomas. 2011. *The Net Effect: Romanticism, Capitalism, and the Internet*. Critical Cultural Communication. New York: New York University Press.

Sunak, Rishi, James Stavridis, and Policy Exchange (Think tank). 2017. *Undersea Cables: Indispensable, Insecure*.

Sunshine, Carl A. 1989. *Computer Network Architectures and Protocols*.

Suzor, Nicolas, Molly Dragiewicz, Bridget Harris, Rosalie Gillett, Jean Burgess, and Tess Van Geelen. 2019. ‘Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online’. *Policy & Internet* 11 (1): 84–103. https://doi.org/10.1002/poi3.185.

The Mentor. 1986. ‘The Hacker Manifesto’. https://web.archive.org/web/20200910085514/http://www.mithral.com/~beberg/manifesto.html. http://www.mithral.com/~beberg/manifesto.html.

Tidy, Jo. 2021. ‘Irish Cyber-Attack: Hackers Bail out Irish Health Service for Free’. *BBC*, 21 May 2021. https://web.archive.org/web/20210908082725/https://www.bbc.com/news/world-europe-57197688. https://www.bbc.com/news/world-europe-57197688.

Tidy, Joanna. 2017. ‘Visual Regimes and the Politics of War Experience: Rewriting War “from above” in WikiLeaks’ “Collateral Murder”’. *Review of International Studies* 43 (1): 95–111. https://doi.org/10.1017/S0260210516000164.

Tompkins, Jane. 1985. *Sensational Designs: The Cultural Work of American Fiction 1790-1860*. New York: Oxford UP.

Tomsen, Peter. 2013. *The Wars of Afghanistan Messianic Terrorism, Tribal Conflicts, and the Failures of Great Powers.* New York: PublicAffairs.

Trottier, Daniel, and Christian Fuchs. 2014. ‘Theorizing Social Media, Politics and the State: An Introduction’. In *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*, 3–38. Routledge Research in Information Technology and Society 16. New York: Routledge.

Tufekci, Zeynep. 2013. ‘“Not This One”: Social Movements, the Attention Economy, and Microcelebrity Networked Activism’. *American Behavioral Scientist* 57 (7): 848–70. https://doi.org/10.1177/0002764213479369.

Turner, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

United States Attorney’s Office. 1995. ‘Fugitive Computer Hacker Arrested in North Carolina’.

https://web.archive.org/web/20130613162729/http://www.justice.gov/opa/pr/Pre_96/February95/89.txt.html. https://www.justice.gov/archive/opa/pr/Pre_96/February95/89.txt.html.

USA Patriot Act (u.s. H.r. 3162, Public Law 107-56). n.d. *1030*. https://www.law.cornell.edu/uscode/text/18/1030.

usTLD. n.d. 'UsTLD Nexus Requirements Policy'. Accessed 21 January 2021. https://www.about.us/policies/ustld-nexus-requirements.

Uzelman, Scott. 2011. 'Media Commons and the Sad Decline of Vancouver Indymedia'. *The Communication Review* 14 (4): 279–99. https://doi.org/10.1080/10714421.2011.624011.

Vallas, Steven P. 2019. 'Platform Capitalism: What's at Stake for Workers?' *New Labor Forum* 28 (1): 48–59. https://doi.org/10.1177/1095796018817059.

Venturini, Tommaso, Liliana Bounegru, Jonathan Gray, and Richard Rogers. 2018. 'A Reality Check(List) for Digital Methods'. *New Media & Society* 20 (11): 4195–4217. https://doi.org/10.1177/1461444818769236.

Vliegenthart, Rens. 2012. 'Framing in Mass Communication Research - An Overview and Assessment: Framing in Mass Communication Research'. *Sociology Compass* 6 (12): 937–48. https://doi.org/10.1111/soc4.12003.

W3C. 2001. 'Stochastic Language Models (N-Gram) Specification'. https://www.w3.org/TR/ngram-spec/.

Warner, Michael. 2010. *Publics and Counterpublics*. 1. paperback ed., 3. print, 4. print. New York, NY: Zone Books.

Wasson, R. Gordon, Albert Hofmann, and Carl A. P. Ruck. 2008. *The Road to Eleusis: Unveiling the Secret of the Mysteries*. 30th anniversary ed. Berkeley, Calif: North Atlantic Books.

Wiener, Norbert. 2007. *Cybernetics or Control and Communication in the Animal and the Machine*. 2. ed., 14. print. Cambridge, Mass: MIT Press.

WikiLeaks. n.d. 'Baghdad War Diary'. Accessed 24 April 2018a. https://wikileaks.org/irq/.

———. n.d. 'WikiLeaks Mirror List'. Accessed 16 June 2020b. https://web.archive.org/web/20110131131742/http://wikileaks.info/.

Wong, Bang. 2010. 'Gestalt Principles (Part 1)'. *Nature Methods* 7 (11): 863–863. https://doi.org/10.1038/nmeth1110-863.

Wood, Michael J., and Karen M. Douglas. 2013. '"What about Building 7?" A Social Psychological Study of Online Discussion of 9/11 Conspiracy Theories'. *Frontiers in Psychology* 4. https://doi.org/10.3389/fpsyg.2013.00409.

Xynou, Maria. 2020. 'Tanzania Blocks Social Media (and Tor?) On Election Day'. OONI. 28 October 2020. https://ooni.org/post/2020-tanzania-blocks-social-media-tor-election-day/.

Xynou, Maria, Simone Basso, Ramakrishna Padmanabhan, and Arturo Filastò. 2021. 'Uganda: Data on internet blocks and nationwide internet outage amid 2021 general election'. OONI. 22 January 2021. https://ooni.org/post/2021-uganda-general-election-blocks-and-outage/.

Zabarenko, Deborah. 2013. 'Hackers Claim Attack on Justice Department Website'. *Reuters*, 26 January 2013. https://web.archive.org/web/20210917084827/https://www.reuters.com/article/net-us-usa-hackers-justice/hackers-claim-attack-on-justice-department-website-idUSBRE90P0H120130126?feedType=RSS&feedName=technologyNews.

https://www.reuters.com/article/net-us-usa-hackers-justice/hackers-claim-attack-on-justice-department-website-idUSBRE90P0H120130126?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29&utm_content=Google+Reader.

Zetter, Kim. 2014. ‘Hacker Lexicon: What Is a Zero Day?’ Wired. 11 November 2014. https://www.wired.com/2014/11/what-is-a-zero-day/.

Zielinski, Siegfried. 2006. *Deep Time of the Media: Toward an Archaeology of Hearing and Seeing by Technical Means*. Electronic Culture: History, Theory, Practice. Cambridge, Mass: MIT Press.

Zuboff, Shoshana. 2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First edition. New York: PublicAffairs.

Zupan, Katja, Nikola Ljubešić, and Tomaž Erjavec. 2019. ‘How to Tag Non-Standard Language: Normalisation versus Domain Adaptation for Slovene Historical and User-Generated Texts’. *Natural Language Engineering* 25 (5): 651–74. https://doi.org/10.1017/S1351324919000366.